مجدى محمد ابو العطا

المرجع الأساسي لمستخدمي

شبكـــات الكمبيوتر

النظرية والتطبيق

الطبعة الأولـــى

١٤٣١هـــ - ٢٠١٠م



المركز الرئيســـى : ٧ ش السخـــاوى – الدور الثانـــــى ت/ف : ٢٤٥١٣٠٠١ – ٢٤٥١٣٠٠٤

مصر الجديـــــدة : ٤٩ ش الحجاز – أمام دار المناسبات ت/ف : ٢٢٤٠٥٣٣٠ – ٢٦٣٩١٢٩٥

مدينة نصـــــر : ١ ش عبد الحكيم الرفاعى من عباس العقاد (أمام الحديقة الدولية)

ت: ٢٦٧٠٢٢٦٣-٢٢٨٧٤٧١١-٢٦٧٠٦٣٢١

المعـــــــارض : ٧ ش السخاوى – روكســــــى (سوق الكمبيوتر ١) ت : ٢٤٥٠١٠٦٣

٤ ش الأسيوطى – روكســـــى (سوق الكمبيوتر ٢) ت: ٢٢٥٨٠٧٧٣

٥٠ ش الخليفة المأمون – روكسى (سوق العصـــر) ت : ٢٢٥٧٧١٢٢

E-mail:info@compuscience.com.eg

www.compuscience.com.eg

رقم الإيداع : ٢٠٠٩/٩٣٢٤
977-389-072-4: I.S.B.N

العلامات التجارية

جميع المصطلحات الواردة بهذا الكتاب مثل أسماء الشركات والبرامج المعروفة كعلامـــات تجارية مثل Microsoft Office ,Excel, Word هى ملك لأصحابها، ونحن نقر بهـــذه العلامات لأصحابها ونحترمها، وإن كنا لم نذكرها صراحة من باب الاختصار.

المرجع الأساسي لمستخدمي شبكات الكمبيوتر

المحتويات في لمحة

المحتويات

مقدمة

إن الحمد لله، نحمده ونستعينه ونستهديه، ونصلى ونسلم على سيدنا محمد صلى الله عليه وسلم وآله وصحبه أجمعين.

{سبحانك لا علم لنا إلا ما علمتنا، إنك أنت العليم الحكيم}...وبعد

أصبحت الشبكات واقعا ملموسا في حياتك. فأنت تتعامل مع الشبكة سواء علمت أم لم تعلم، فأنت حينما تتصل من منزلك بأحد أصدقائك تستخدم شبكة تليفونات ويتم الاتصال بينك وبين صديقك من خلال شبكة. والجهاز الذي تسحب منه نقودك في البنك أو حتى في الأماكن العامة يستخدم شبكة اتصال، والبريد الالكتروني وتصفح الويب يتم عن طريق شبكة الانترنت العالمية. وهكذا ترى أن شبكات البيانات مثلها مثل أجهزه الكمبيوتر أصبحت جزءا لا يتجزأ من حياتنا .

وفي هذا الكتاب سوف تتعلم في خطوات سهلة أحدث ما توصل إليه العلم في كل ما يتعلق بالشبكات حيث يشرح للمبتدئين بطريقة ممتعة وشيقة، معلومات أولية ومفاهيم أساسية عن الكمبيوتر ونظم الأعداد وأنواع الشبكات ويتناول بالشرح نموذجي **OSI** و **TCP/IP** ونظم تشغيل الشبكات بالإضافة إلي تقنيات الشبكات المحلية ومكوناتها وكيفية تجميعها. كما يشرح للمتمرسين ومديري الشبكات بلغة سهلة مفاهيم متقدمة عن أمان الشبكات ، وإدارتها، والشبكات الواسعة (**WAN**) والشبكات اللاسلكية (**WLAN**)، وكيفية عنونة **IP**، وتقنية الموجه (**Router**) والشبكات الفرعية (**Subnetting**) وشبكات **VPN**.

ولهذا فإننا نعتقد أن هذا الكتاب يحقق فائدة عالية لكل من المبتدئين من ناحية والمتمرسين ومديري الشبكات من ناحية أخري.

إن هذا الكتاب الذي بين يديك هو دليل متكامل أكاديمي وعملي لكل من يرغب في إدارة شبكة كبيرة، أو إنشاء شبكة صغيرة ، أو ربط عدد محدود من أجهزة الكمبيوتر في شبكة واحدة .

ولأن هذا الكتاب أُعد كمرجع فأنت لست ملزماً بقراءة الكتاب من الجلدة إلي الجلدة لكي تفهم شبكات الحاسب ، وإنما يمكنك قراءة الموضوع الذي تحتاج إليه إلا أننا نفضل أن تقرأ الأبواب الثلاثة الأولي بترتيبها الوارد بالكتاب.

لمن هذا الكتاب

رغم أن هذا الكتاب أُعد خصيصاً لطلبة المعاهد والجامعات، إلا أنه يصلح لكل من يرغب في تعلم كيفية بناء الشبكات وتشغيلها بغية الحصول علي وظائف مرموقة بمرتبات عالية.

يبدأ الكتاب بمراجعة المفاهيم الأساسية ، ويستخدم طريقة تعليم تطبيقية لتوضيح المفاهيم الرئيسية لموضوعات الكتاب. وعند الضرورة يتم استخدام أمثلة مفصلة وشروح واضحة تشتمل علي الكثير من الرسومات التخطيطية لتحقيق الاستفادة القصوى من الشرح .

يركز هذا الكتاب علي المفاهيم والمعلومات الأساسية التي تؤهلك لكي تصبح مهندس شبكات ناجح ، و يؤهلك للتقدم لاختبار شهادة

Microsoft Certified Systems Engineer (MCSE)

وشهادة **Cisco Certified Network Association (CCNA)**

عموماً يخاطب هذا الكتاب الفئات الآتية

- مستخدمو أجهزة الكمبيوتر الشخصية.
- أصحاب المعاهد والجامعات الراغبين في إنشاء شبكات واستخدامها.
- طلاب المعاهد والجامعات الذين ينشدون سياسة خطوة ..... خطوة أو التعلم الذاتي.
- مهندسو الشبكات والمسئولون عن إدارة الشبكات وتأمينها.
- الطلاب والمهندسون الذين يرغبون في الحصول علي شهادة مهندس شبكات تؤهلهم لوظائف مرموقة.

ترتيب الكتاب

لقد حرصت على عرض المادة بأسلوب شيق وسهل وميسر متوخياً تحقيق الأهداف المرجوة بشكل أفضل وأنجح. أما ترتيب الكتاب فقد جاء على النحو التالي :

في الباب الأول : قدمت مقدمة إلي الشبكات استغرقت أربعة فصول، بدأتُ في الفصل الأول بإعطاء خلفية ضرورية شملت تعريف الشبكة وفوائدها والقيود التي تفرضها علي المستخدمين وفي الفصل الثاني والثالث الأساسيات التي يجب أن تعرفها عن الحاسب وشملت الأجهزة والبرامج ونظم الأعداد وكيفية حساب سرعة نقل البيانات وفي الفصل الرابع شرحت أنواع توصيل الشبكات وأنواع الشبكات ثم تعرضت لتصنيف الشبكات الحديثة.

وفي الباب الثاني: شرحت المفاهيم الأساسية لربط الشبكات في ثلاثة فصول. بدأت في الفصل الخامس بشرح المواصفات القياسية والتقنية للشبكات المحلية وركزت علي تقنية Ethernet وتقنية Token Ring و FDDI وتقنية ATM بالإضافة إلي تقنية ربط شبكات المنازل ومقياس PPP. وفي الفصل السادس شرحت النموذج المرجعي للانتقال بين الأجهزة OSI وكيفية تحرك البيانات في الشبكة ونقل البيانات في النموذج وفي الفصل السابع شرحت نموذج TCP/IP وعرضت لمقارنة نموذج OSI بالنموذج TCP/IP.

وفي الباب الثالث: شرحت مكونات الشبكة علي مدي ثلاثة فصول ففي الفصل الثامن شرحت أجهزة ووسائط الاتصال بالإضافة إلي أنواع الكابلات ومواصفاتها ، وفي الفصل التاسع شرحت وظيفة وحدة الخدمة (Server) والخدمات الشائعة لوحدة الخدمة المخصصة بالإضافة إلي مجموعات RAID، وفي الفصل العاشر شرحت نظم تشغيل الشبكات بالإضافة إلي نظم تشغيل الشبكات النظيرة.

وفي الباب الرابع : شرحت كيفية إنشاء الشبكات في ثلاثة فصول. بدأت في الفصل الحادي عشر بشرح التخطيط لبناء الشبكة وإتباع أفضل الممارسات ، وفي الفصل الثاني عشر كيفية تجميع الشبكة واختبار صحة تثبيتها ، وفي الفصل الثالث عشر تقنيات الاتصال بالانترنت وخطوط الاتصال T1 و T3 السريعة.

وخصصت الباب الخامس : لشرح ربط شبكات Microsoft علي مدي ثلاث فصول شملت إعداد شبكات Windows Vista والاتصال بالشبكات ومشاركة موارد الشبكة.

وخصصت الباب السادس: لشرح تقنية التوجيه والشبكات الفرعية في ثلاث فصول، شرحت في الفصل السابع عشر كيفية عنونة IP، وشرحت الحاجة إلي عناوين إضافية عن طريق تقنيات جديدة مثل عنونة IPv6 أو CIDR ، ثم شرحت توصيف وحدة الخدمة والوحدات التابعة باستخدام إعدادات IP الثابتة، وأخيرا استخدام بروتوكول DHCP لتعيين عناوين ديناميكية للشبكة. وفي الفصل الثامن عشر شرحت التوجيه والموجهات وتناولت كيفية نقل حزم البيانات علي الشبكة والفرق بين التحويل والتوجيه. وما هي جداول التوجيه وبروتوكولات التوجيه ، وخصصت الفصل التاسع عشر لشرح كيفية

عمل التشبيك الفرعي وأهميته، وكيفية تأسيس قناع الشبكة الفرعية وتطبيقه.

أما الباب السابع: فهو موجه لمدير الشبكة حيث بدأت في الفصل العشرين بشرح مهام إدارة الشبكة وفي الفصل الحادي والعشرين أوضحت عوامل مساعدة في إدارة الشبكة وتعرضت في الفصل الثاني والعشرين لمشكلات الشبكة وإصلاحها.

وفي الباب الثامن : تحدثت عن أمان الشبكة، ففي الفصل الثالث والعشرين شرحت تأمين الشبكة وحمايتها من الفيروسات والقراصنة وفي الفصل الرابع والعشرين حماية البيانات علي الشبكة وتأمين الشبكات اللاسلكية، وفي الفصل الخامس والعشرين جدران النار وكيفية عملها .

وفي الباب التاسع والأخير : شرحت التقنيات المتطورة في الشبكات في ثلاثة فصول، بدأت في الفصل السادس والعشرون بشرح الشبكات الواسعة (WAN) ومكوناها ومن يحتاجها،

وفي الفصل السابع والعشرون الشبكات اللاسلكية (WLAN) وكيفية تشكيلها والتهديدات التي تواجها، وفي الفصل الثامن والعشرون شرحت نظرة عامة علي شبكات VPN وأنواعها وفوائدها واستراتيجيات تطبيقها وكيفية العمل علي تمرير البيانات عبر أنفاق وصيغ التشفير .

وفي نهاية الكتاب وضعت ثلاثة ملاحق : الملحق الأول لبطاقات مرجعية تشتمل علي معلومات مختصرة ومفيدة، والملحق الثاني لإجابات الأسئلة الواردة بفصول الكتاب، والملحق الثالث لأهم مصطلحات الشبكات التي تهم العاملين في المجال.

وبعد ... عزيزى القارئ نتركك الآن لتقليب صفحات الكتاب آملين أن تجد المتعة والفائدة التي تنشدها .

{وآخر دعوانا أن الحمد لله رب العالمين}.

مجدي محمد أبو العطا

الباب الأول

مقدمة إلي الشبكات

الفصل الأول : نظرة عامة علي ربط الشبكات

الفصل الثاني : أساسيات الكمبيوتر

الفصل الثالث : أساسيات الكمبيوتر "نظرة موسعة"

الفصل الرابع : أنوا ع الشبكات



في هذا الفصل نلقى نظرة عامة على مفهوم الشبكة ولماذا نلجأ إليها ومكوناتها والقيود التى تفرضها الشبكات على المستخدمين........الخ.

وفيما يلي من بقية فصول الكتاب ستتعرف بالتفصيل على المفاهيم والمصطلحات الواردة. بالانتهاء من هذا الفصل ستتعرف على :

- *مقدمة*
- *تعريف الشبكة*
- *لماذا نلجأ إلى الشبكات*
- *القيود التي تفرضها الشبكات على المستخدمين*
- *مكونات الشبكة*
- *مدير الشبكة*

حينما ظهرت الاختراعات البخارية التى سجلها العلماء فى بدايات القرن الثامن عشر الميلادى، وقتها وقف الناس مبهورين مندهشين ثم متحسرين على من سيأتى بعدهم من الأجيال. لأن من سيأتى بعدهم لن يجد شيئا يخترعه بعد. فهم–على ظنهم–لم يبقوا للآخرين علما إلا استنفذوه، ولا اختراعا إلا أنجزوه. واليوم فان كل ما اخترعوه قد أصبح نسيا منسيا. وإن بقى منه شيء فقد دخل المتاحف كأثر كاد أن ينسى.

وجاء اختراع الكمبيوتر فى النصف الأخير من القرن العشرين. وتمركزت أنظمة الكمبيوترات خلال العقود الأولى من اختراعها فى غرفة واحدة كبيرة، تحتوى على أجهزة ضخمة ووحدات تخزين كبيرة قليلة السعة. وجأت فكرة إنتاج الكمبيوترات. بحجم الطابع البريدى وتصنيعها بكميات كبيرة. بعد أن كانت خيالا محضا خلال العشرين سنة الماضية، فأزاحت مركز الكمبيوتر الذى يتألف من غرفة تحتوى على كمبيوتر ضخم، وأحلت محله مجموعة من الكمبيوترات التى تؤدى مهام مستقلة عن بعضها مع الحفاظ على التخاطب فيما بينها عبر ما يسمى بشبكة الكمبيوتر. فزادت الدهشة وانعقد اللسان وقال الناس :وماذا بعد؟ وأصبح الجيل الحالى ينظر بإشفاق إلى هذه المحاولات البدائية لاستخدامات الكمبيوتر فى القرن الماضى. وكان للمزج بين تقنية الكمبيوترات والاتصالات أثرا مهما فى بلوغ الطريقة التى تصمم بها الكمبيوترات حالياً. إن التقدم التكنولوجي السريع في صناعة الكمبيوترات والذي ميزها عن غيرها من الصناعات كصناعة السيارات أو الطائرات بالإضافة إلي المقدمات التى طرأت على التقدم التكنولوجى مثل إرساء الشبكات الهاتفية العالمية الثابتة والمتحركة، وإطلاق الأقمار الصناعية.كان لهذه التطورات بالإضافة إلى تضخم الشركات وظهور الشركات متعددة الجنسيات وافتتاح فروع لها فى أماكن جغرافية متباعدة. أبلغ الأثر فى البحث عن نظام يؤمن الاتصال بين الكمبيوترات. وظهرت الحاجة لتأمين إمكانية الاتصال بين الكمبيوترات بشكل غير معقد. وإذا كنا قد قلنا فى البداية أن اختراع الكمبيوتر يعتبر أهم ما ظهر فى القرن العشرين، فان الجزء الخاص بربط أجهزة الكمبيوتر، وتشكيلها مع بعضها البعض، وعلم الشبكات هو من أكثر هذه العلوم أهمية فى وقتنا الراهن. إن اهتمام الناس بالسعى للتواصل والارتباط عبر الشبكات المختلفة ولاسيما

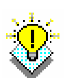
شبكة الانترنت، قد أسهم بشكل كبير فى لقاء الحضارات وتواصل البشرية بمختلف أجناسها فيما بينهم، ليصبح العالم فعلاً قرية صغيرة.

إن تصميم واستخدام وتنظيم شبكات الكمبيوتر هو موضوع هذا الكتاب وقد جاء اهتمامنا بهذا الموضوع لأن شبكات الكمبيوتر تعتبر حقلاً غنيا وواعدا فى بلادنا ومازال يحتاج الكثير من الجهد والعمل والخبرات.

تعريف الشبكة

كلمة شبكة تعنى باختصار توصيل جهازين أو أكثر من أجهزة الكمبيوتر ببعضهما ويتم ذلك عن طريق التوصيل المادي ويشمل توصيل الكابلات المادية واستراتيجيات التوصيل اللاسلكي بالإضافة إلى البرامج التي تلزم لإتمام عملية الاتصال. ويمكن أن تكون الشبكات بسيطة مثل تمكين جهازي كمبيوتر متصلين بكبل متسلسل من الاتصال ببعضها، كما يمكن أن تكون معقدة مثل شبكات الاتصال الواسعة كتلك التي تستخدمها شركات الطيران العالمية.

وهناك مجموعة من المتطلبات التي يجب تحققها حتى تتمكن أجهزة الكمبيوتر من الاتصال ببعضها عبر شبكة الاتصال. أول هذه المتطلبات هي البرامج التي تسمح باتصال البيانات. وكذلك يجب أن تكون أجهزة الكمبيوتر داخل الشبكة قادرة على التعرف على بعضها البعض. كما يجب أن تكون هناك طريقة قياسية للتعرف على الأجهزة المتصلة بالشبكة .



إذا كنت لا ترغب في استخدام كابلات، تستطيع إنشاء شبكة لاسلكية. فى هذا النوع من الشبكات، يتم تثبيت كارت خاص بالشبكة اللاسلكية، مزود بجهاز معدني لاستقبال وإرسال الإشارات الكهرومغناطيسية فى كل جهاز كمبيوتر. بذلك تتمكن أجهزة الكمبيوتر من الاتصال معاً بدون استخدام الكابلات.

لماذا نلجأ إلى الشبكات

هناك أسباب عديدة لربط شبكات الكمبيوتر. فحيثما كانت الحاجة إلى مشاركة البيانات

أو البرامج، فإن ربط الشبكات هو الحل الأمثل. ولا يشترط أن يتم بناء الشبكات بواسطة شركات كبيرة أو مؤسسات عالمية فقد يكون لدى شخص مكتب صغير به جهازي كمبيوتر واتصال DSL أو كبل ويرغب في تمكين الوصول إلى الانترنت لكل موظفيه.

ويمكن اختصار الأسباب التي نلجأ إليها لإنشاء الشبكات فيما يلي :

أولا: مشاركة الموارد:

ونعني بها استخدام وسائط تخزين مشتركة وملفات مشتركة وتطبيقات مشتركة وطابعات مشتركة وتفصيل ذلك على النحو التالي

- استخدام وسائط تخزين مشتركة: حيث يمكن لجميع مستخدمي الشبكة استخدام نفس البيانات الموجودة على القرص المغناطيسي والفائدة من ذلك أنك تستغني عن تركيب قرص صلب في كل جهاز كمبيوتر كما أنك تستطيع استخدام الملفات والتطبيقات الموجودة على نفس القرص بسهولة.
- مشاركة الملفات : تخيل الحياة بدون شبكة عندما تريد نقل ملفات بين أجهزة كمبيوتر غير متصلة ببعضها. ماذا ستفعل؟ ستضطر إلى نسخ الملف إلى قرص مغناطيسي وتنتقل به إلى جهاز آخر ثم تقوم بنسخ الملف إلى هذا الأخير. لا شك أن هذه الطريقة لا تعد فعالة لنقل البيانات أو إدارتها فهي أيضا مستهلكه للوقت ولا يمكن الاعتماد عليها. المشكلة في هذه الطريقة أن الإصدارات لدى المستخدمين قد تختلف من مستخدم لآخر نتيجة للتحديث الذي يحصل باستمرار على الملفات والبيانات. وهذا يؤدى إلى إرباك وأخطاء فادحة في العمل. تخيل مثلا أنك تستخرج مرتب لموظف بدون إضافة آخر علاوة حصل عليها. ماذا يمكن أن يحدث؟
- مشاركة التطبيقات : من الأفضل وضع البرامج أو التطبيقات على محرك أقراص، ومشاركة هذا المحرك بين جميع المستخدمين بدلا من وضعها على كل جهاز على حدة. إن شراء نسخة واحدة من البرنامج ثم وضعها على محرك أقراص مشترك على الشبكة بحيث يتمكن كل مستخدم من الاتصال بها يستلزم شراء ترخيص يسمح لجميع المستخدمين الموجودين على الشبكة باستخدام البرنامج . بدون استخدام شبكة لا يستطيع جميع

المستخدمين العمل على تطبيق واحد مثل برنـــامج **Microsoft Office** أو بـــرامج المخازن أو الحسابات .

- استخدام طابعات مشتركة: بدون استخدام شبكة اتصال ستخصص لكل مستخدم داخل المؤسسة طابعة مستقلة أو تضطر لاستخدام علب رموز التبديل اليدوية. وهذه العلب هي التي تحدد أي منفذ طابعة كمبيوتر يتصل بالطابعة. لا يخفى عليك الإرهاق المالي الـــذي تسببه هذه الطريقة. استخدام طابعة مشتركة يوفر هذا العناء و يسمح لجميع مستخدمي الشبكة باستخدام نفس الطابعة.

ثانيا: سهولة استخدام الانترنت:

وجود شبكة اتصالات تسمح بتوصيل جميع المستخدمين داخل الشبكة بالانترنت من خلال اتصال واحد.لا شك أن هذا يقلل تكاليف حسابات الانترنت. في الحقيقة بدون الـــشبكة يحتاج كل مستخدم للاتصال بالانترنت عن طريق خط اتصال خاص به. هذا معناه أنه لن تكون هناك انترنت.

ثالثا: سرعة الاتصال:

توفر الشبكة الوقت وتزيد سرعة العمل . تخيل بدون شبكة أنك تترك مكانك لتنتقل حيث تريد نسخ الملف أو تبديل الرمز الموصل إلى جهازك من علبة رموز التبديل لطباعة تقرير. باستخدام الشبكة سوف توفر هذا الوقت .

رابعا: مركزية البيانات:

إذا لم تكن تستخدم شبكة. لا يمكنك التحكم في أجهزة الكمبيوتر وإدارتها بكفاءة عاليـــة والتأكد من أنها تشترك في توصيفات عامة. كما أنك لا تستطيع أن تتعرف على البيانـــات الموجودة على كل منها.

استخدام الشبكة يوفر مركزية وظائف الإدارة وتوحيد برامج التطبيقات. كمـــا يمكنـــك استخدام الأدوات المساعدة التي تمكنك من تشخيص المشكلات وإصلاحها ومـــن أمثلـــة الأدوات المساعدة برامج اكتشاف الفيروسات وإزالتها، وبرامج اكتـــشاف الأعطـــال، وبرامج إدارة الشبكة ......الخ .

القيود التي تفرضها الشبكات على المستخدمين

- لا يمكن حذف الملفات بصورة عشوائية، فقد تكون هذه الملفات خاصة بمستخدمين آخرين.
- لابد من استخدام اسم مستخدم وكلمة مرور لتتمكن من الوصول إلى الملفات الموجودة على وحدة الخدمة. يعد استخدام اسم المستخدم وكلمة المرور واحداً من النظم التأمينية التى تستخدمها الشبكات.
- حين ترسل تقريراً أو بياناً للطباعة على الطابعة المشتركة، يجب عليك الانتظار حتى يأتى دورك فى طابور الانتظار على الطابعة. إذا كان واحداً أو اثنين من المستخدمين أرسلوا طلباتهم إلى الطابعة قبلك. فلابد من الانتظار بعض الوقت.
- ربما تنتظر أيضا إذا أردت استرجاع أحد الملفات وكان هذا الملف قيد الاستخدام بواسطة زميل آخر على الشبكة.
- إذا أصيب أحد الأجهزة (الوحدات التابعة) بفيروس، فربما ينتقل إلى جميع الأجهزة المرتبطة بالشبكة.
- لا تستطيع الوصول إلى ملف موجود على جهاز آخر داخل الشبكة إلا إذا كان مفتوحاً ومتاحاً، فإذا كان صاحب الجهاز أغلقه لسبب ما. فعليك الانتظار أو معرفة كلمة المرور الخاصة به.

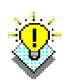
مكونات الشبكة

تشتمل الشبكة في ابسط مكوناتها علي جزئين. الجزء الأول هو الشبكة المادية وتشمل الأسلاك وبطاقات الشبكة وأجهزة الكمبيوتر نفسها والمعدات الأخرى التي تستخدمها الشبكة لنقل البيانات. والجزء الثاني هو البرامج التي تسير أو تقود الأجهزة المادية. يمكن تشبيه الأجهزة المادية بالسيارة التي تتكون من الموتور والشاسيه ودائرة الكهرباء .... الخ، ويمكن تشبيه البرامج بالبنزين الذي بدونه ستبقي السيارة رابضة مكانها ولن تتمكن من السير .

وفيما يلي نلقي الضوء باختصار علي مكونات الشبكة لأننا سنتحدث عن كل من الشبكة المادية والبرامج بالتفصيل في الفصول التالية

الشبكة المادية:

هي كل ما يمكن لمسه باليد مثل أجهزة الكمبيوتر والأسلاك وبطاقات الشبكة والطابعات. باختصار هي كل الأجهزة التي تمكن الشبكة من العمل وهي :



رغم أن ربط الشبكات اللاسلكية يجعل الاتصال المادي بين أجهزة الشبكة يبدو غير واقعي بعض الشئ ، فإن التخطيط الكلي للشبكة لا يختلف بين الشبكات التي تستخدم الأسلاك والشبكات اللاسلكية.

١. وحدة الخدمة(Server): تستخدم معظم الشبكات جهاز مستقل للعمل كوحدة خدمة مخصص فقط لتوفير موارد مشتركة مثل الأقراص الصلبة والطابعات، حتى يتسنى لأجهزة الكمبيوتر التابعة على الشبكة (Work Stations) الوصول إلى هذه الموارد. تسمى وحدة الخدمة فى هذه الحالة "وحدة خدمة مخصصة" لأنها مخصصة لتوفير خدمات الشبكة المشتركة. وبالرغم من ذلك، تسمح بعض الشبكات الصغيرة لأى جهاز على الشبكة بالعمل كوحدة خدمة وجهاز تابع فى نفس الوقت. تسمى هذه الشبكات "شبكات تناظرية". أو شبكة الند للند (سنعود لشرح وحدة الخدمة بالتفصيل في الفصل التاسع)
٢. محطة العمل أو الوحدة التابعة (Workstation): هي جهاز الكمبيوتر الذي يستخدمه الشخص المرتبط بالشبكة. لايتم عادة مشاركة هذه الأجهزة بين جميع المستخدمين.
٣. كروت الشبكة (NIC)Network Interface Card: يوجد داخل كل جهاز كمبيوتر متصل بالشبكة كارت خاص عبارة عن دائرة الكترونية يطلق عليه "كارت الشبكة" ويعرف بـــNIC. يمكن أن يتم تركيب كارت الشبكة على اللوحة الأم كما يمكن أن يكون موجوداً ضمن مكونات اللوحة الأم. لمزيد من التفاصيل راجع الفصل الثامن
٤. وحدة التوصيل (hub):وهو عبارة عن جهاز صغير يحتوى على مجموعة من موصلات

الكابلات، يتصل به كل جهاز فى الشبكة بكابل منفصل. ويربط بين جميع الأجهزة . تستخدم بعض الشبكات جهازا أسرع منhub يعرف بالسويتش(Switch)وكثير ما يحدث خلط فيستخدم تعبيرhub للإشارة إلى جهاز hub أو جهاز سويتش. (راجع الفصل الثامن لمزيد من المعلومات عن كل من الـ Hub والـ Switch)

٥. **الأسلاك والكابلات (Cables) : رغم أن كلا من الأسلاك والكابلات لا تعتبر أجهزة. إلا إننا أوردناهما هنا لأهميتهما لأنهما يجب أن تخضعا لمقاييس صارمة حتي تعمل الشبكة بطريقة صحيحة. يستخدم الكابل لربط أجهزة الكمبيوتر معا ويتم إدخال هذا الكابل فى كارت الشبكة المثبت فى جهاز الكمبيوتر من الخلف. تستخدم الشبكات القديمة نوع من الكابلات يطلق علي Coaxial (كابل متحد المحور). بينما تستخدم الشبكات الحديثة كابل يسمى Twisted Pair (الكابل المزدوج الملفوف) وهو الأفضل فى الشبكات الحديثة والأكثر استخداما. سنعود لشرح الأسلاك والكابلات وأنواعها في الفصل الثامن بإذن الله.**

٦. **الموجه (Router) : الموجهات أجهزة تنقل البيانات بين الشبكات . لذا يجب توصيل الموجهات بشبكتين علي الأقل. في شبكات الاتصال تعرف الموجهات أفضل مسارات التوجيه لنقل البيانات من نقطة إلي نقطة أخري داخل الشبكة. (لمزيد من المعلومات عن الموجهات راجع الفصل الثامن عشر)**

٧. **الطابعة (Printer) : يمكن لأكثر من مستخدم إرسال ما يرغب في طباعته إلي الطابعة المتصلة بالشبكة.**

نظام تشغيل الشبكة

لا يمكن أن تعمل الشبكة بدون نظام تشغيل يوجه المكونات المادية ويوفر لمدير الشبكة الوسائل التى تمكنه من إدارة الشبكة بصورة صحيحة. فى حالة الشبكات التناظرية العاملة بنظام Windows، يتم تشغيل الشبكة من خلال الإمكانيات المتاحة فى نظام Windows أما عند استخدام نظام تشغيل خاص بالشبكات مثل نظام Netware أو نظام Windows Server 2003/2008 فإن الأمر يختلف . من أكثر نظم تشغيل الشبكات

استخداما نظام **Netware** ونظام **Windows Server 2003/2008**.

- نظام **Netware** من إنتاج شركة **Novell** وهو من أكثر نظم التشغيل استخداماً. وهو نظام معقد بالقياس إلي نظام **Windows** .
- أما نظام **Windows 2003/2008 Server** فهو نظام تشغيل من أنتاج شركة **Microsoft** وهو مصمم للعمل علي وحدات الخدمة (**Server**) وهو نظام سهل سواء في الإعداد أو الاستخدام مقارنة بنظام **Netware**.
- بالإضافة إلي نظم التشغيل الأخرى **Linux** و **Unix**

مدير الشبكة

من المهم تعيين مدير للشبكة (وإن كانت صغيرة الحجم) لضمان استمرار الشبكة فى العمل بشكل جيد. يقوم مدير الشبكة بعدة مهام مثل ضمان توافر مساحة كافية على وحدة خدمة الملفات. والتأكد من نسخ الملفات بصورة منتظمة وتمكن الموظفين الجدد من الدخول إلى الشبكة عن طريق تعيين اسم مستخدم وكلمة مرور لكل منهم. كما ينبغي على مدير الشبكة حل المشكلات التي يعجز المستخدمون عن حلها. وأن يكون قادرا على تحديد المواقف التي تستدعى الاستعانة بالخبراء.

ملخص الفصل

شرحنا في هذا الفصل المقصود بالشبكة ثم شرحنا فوائد استخدام الشبكات. شرحنا أيضا القيود التي تفرضها الشبكات على المستخدمين. ثم ألقينا نظرة خاطفة على مكونات الشبكة ، وأخيراً شرحنا المقصود بكل من نظام تشغيل الشبكة ومدير الشبكة .

تدريبات

١. يمكن تعريف شبكة الاتصالات على أنها:

أ. أجهزة كمبيوتر موجودة في أماكن متفرقة .

ب. مجموعة من العناصر (أجهزة وبرامج) يتم ربطها معاً لتمرير المعلومات.

ج. أجهزة تعمل بدون حاجة لبرامج لتشغيلها.

٢. من مزايا استخدام الشبكات.

أ. تخصيص طابعة مستقلة لكل مستخدم داخل المؤسسة.

ب. استخدام نفس الملفات والتطبيقات الموجودة على أحد الأجهزة بواسطة باقي المستخدمين.

ج. تمكين جميع المستخدمين داخل الشبكة من الاتصال بالانترنت من خلال اتصال واحد.

٣. اختر الإجابة الصحيحة

أ. تسمح الشبكات لأي شخص من غير العاملين بالوصول إلى الملفات الموجودة على وحدة الخدمة.

ب. لابد أن تسأل قبل حذف أحد الملفات هل يخص مستخدم آخر أم لا ؟

ج. يجب عليك أن تنتظر حتى يأتي دورك في طابور الانتظار على الطابعة قبل أن تطبع ملف يخصك.

٤. أذكر أربعة من أهم المكونات المادية لشبكة الاتصالات.

٥. أذكر اثنين من أهم نظم تشغيل الشبكات.

٦. من مهام مدير الشبكة:

أ. مراقبة حضور وانصراف الموظفين.

ب. ضمان توفير مساحة كافية على وحدة الخدمة.

ج. تعيين اسم مستخدم وكلمة مرور لجميع المستخدمين.

د. حل مشكلات الشبكة والإجابة على استفسارات المستخدمين.





نشرح في هذا الفصل مدخل إلى علم الكمبيوتر حيث نتناول مكونات الكمبيوتر الأساسية وهي الأجهزة والبرامج ثم نشرح بشئ من التفصيل الأجهزة التي يتكون منها الكمبيوتر والبرامج التي تسير هذه الأجهزة .

بانتهاء هذا الفصل ستتعرف على:

- *المكونات المادية للكمبيوتر*
- *برامج الكمبيوتر*

أعلم أنك تعرف الكثير عن أساسيات الكمبيوتر كمدخل لعلم الكمبيوتر من دراستك أو معلوماتك السابقة. ولكننا هنا فى هذا الكتاب نشرح بصفة خاصة شبكات الكمبيوتر. ولأن شبكات الكمبيوتر تتكون من أجهزة كمبيوتر. فكان من الضروري أن نوضح نبذه مختصرة عن مفاهيم الكمبيوتر الأساسية. ولأن كل جهاز كمبيوتر يعمل بنفس الطريقة التى تعمل بها أجهزة الكمبيوتر الأخرى على الشبكة، فإن فهم طريقة عمل جهاز الكمبيوتر سيساعدك بالقطع علي فهم كيفية عمل الشبكات.

(إذا فهمت جيداً كيف يعمل جهاز الكمبيوتر، ستفهم بسهولة كيفية ربط الشبكات وطريقة عملها).

مكونات الكمبيوتر

حتى يمكن تشغيل البيانات علي الكمبيوتر والاستفادة منها، لابد من وجود مكونات مادية (أو أجهزة) وبرامج لتتولي توجيه هذه الأجهزة ومن ذلك يتضح أن المكونات الرئيسية للكمبيوتر هي:

- الأجهزة أو المكونات المادية (Hard Ware)
- البرامج (Soft Ware)

وفيما يلي نلقي الضوء علي تلك المكونات بشئ من التفصيل

أولاً: الأجهزة (Hard Ware)

تقصد بالأجهزة المكونات المادية التي يتكون منها جهاز الكمبيوتر ، وهي كل ما يمكن لمسه باليد، مثل الصندوق الخارجي ولوحة المفاتيح والأقراص المغناطيسية والبطاقات المختلفة مثل بطاقة الفيديو وبطاقة الشبكة وبطاقة الصوت ..... الخ .

فيما يلي سوف نلقي نظرة خاطفة علي أهم المكونات المادية التي لها صلة بموضوع الكتاب دون الخوض في المكونات البسيطة مثل لوحة المفاتيح والطابعة والفأرة وشاشات العرض. باعتبارها معلومة للجميع بالضرورة. إذا رأيت أنك تحتاج لفهم هذه الأجهزة يمكن مراجعتها من دراستك السابقة أو الرجوع لكتابنا "تعرف على الكمبيوتر الشخصي". عندما نري ضرورة للتركيز علي شرح أحد هذه المكونات بالتفصيل لأن له علاقة بموضوع

الكتاب. سنتوسع في الشرح حسب ما تقتضيه الضرورة. وعندما نري أنـــه لا ضـــرورة لشرح تفصيلات عن أحد المكونات سنمر عليها مرور الكرام أو سنتخطاها إلي التالية.

سنركز في هذا الفصل علي المكونات التالية

- الصندوق الخارجي Case
- الذاكرة Memory
- المنافذ/المخارج Ports
- مصدر الطاقة Power Supply
- الأقراص المغناطيسية Hard Disk
- اللوحة الأم Mother Board
- فتحات التوسعة Expansion Slots
- المعالج Processor
- كروت التوسعة Expansion Cards

الصندوق الخارجي للكمبيوتر Case

بصفة عامة فأن الـــ Case عبارة عن غطاء خارجي صلب مـــصمم بفتحاتـــه الأماميـــة والخلفية بحيث يتم تثبيته حول مكونات الكمبيوتر من كروت وكابلات وغيرها بينما تظهر فى الجوانب فتحات لتثبيت المكونات التى يحتاجها المستخدم مثل فتحة مـــشغل القـــرص المدمج CD-ROM أو القرص المرن التى تظهر بالأمام أو منفذ بطاقة الصوت الذى يظهر من الخلف. يوجد بالصندوق الخارجى للكمبيوتر الآلي مجموعة من الأزرار واللمبات التى تمكنك من التحكم فى تشغيل الجهاز

المنافذ/المخارج Ports

المنفذ هو فتحة توصيل خارجية موجودة فى الجانب الخلفى للصندوق Case، ويمكن عن طريقها توصيل أجهزة ومكونات خارجية لنقل البيانات والأوامر بينها وبين الكمبيـــوتر، تظهر المنافذ/المخارج(Ports) خلف جهاز الكمبيوتر.

- المنفذ المتوالى Serial Port: يحتوى منفذ التوالى على ٩ أو ٢٥سن توصيل، وعن طريق هذا النوع من المنافذ يتم توصيل الفأرة والمودم والماسح الضوئي ولوحة المفاتيح، حيـــث تقوم منافذ التوالى بإرسال نبضة واحدة من البيانات فى كل مرة عبر الكابل المتصل بها(أي بطريقة متوالية أو متتابعة) ويمكنها إرسال البيانات بمسافة تزيد عن ٢٠ قدم. كما يحتوى

الكابل المستخدم مع المنافذ المتوالية على ٩ أو ٢٥ فتحة لتثبيته مع المنفذ، يقوم الكمبيوتر بتسمية المنافذ المتوالية على التوالي بالاسم **COM** مضافاً إليه رقم للتمييز، ويسمى المنفذ المتوالي الأول **COM1** والثانى **COM2** وهكذا.

- **المنفذ المتوازى (Parallel Port)**: المنفذ المتوازى هو فتحة اتصال تحتوى على ٢٥سن للتوصيل، وعن طريق هذا النوع من المنافذ يتم توصيل الطابعة وجهاز تشغيل الشرائط، وتتميز المنافذ المتوازية بأنها أسرع فى نقل البيانات من نظيراتها على التوالى حيث تقوم بإرسال ٨ نبضات من البيانات على الأقل فى كل مرة عبر الكابل المتصل بها وعلى النقيض لا يمكنها إرسال البيانات لمسافة تزيد عن ٢٠ قدم. كما يحتوى الكابل المستخدم مع المنافذ المتوازية على ٢٥ سن للتثبيت فى المنفذ.

يقوم الكمبيوتر بتسمية المنافذ المتوازية بالاسم **LPT** مضافة إليه رقم التمييز ويسمى المنفذ المتوازى الأول **LPT1** والثانى **LPT2** وهكذا ومن أمثلتها منفذ توصيل الطابعة.

مصدر الطاقة Power Supply

مصدر الطاقة عبارة عن محول يقوم بتحويل التيار الكهربائي العادي المستخدم فى المنازل والمكاتب مثلاً والذي يطلق عليه **AC** إلى الطاقة التى يحتاجها الكمبيوتر. وتقاس مقدرة مصدر التيار بالوات **Watt**، حيث عادة ما تستهلك أجهزة الكمبيوتر طاقة كهربائية ضئيلة جداً. فعلى سبيل المثال فإن كمية الطاقة التى تستهلكها ٧ أجهزة كمبيوتر تعادل تلك التى يستخدمها مجفف واحد للشعر. وتحتاج معظم أجهزة الكمبيوتر إلى مغذى تيار بقدرة ٢٥٠ وات تزداد إلى ٤٠٠ وأكثر فى حالة وحدات الخدمة **Servers** حسب تعليمات الجهة الصانعة.

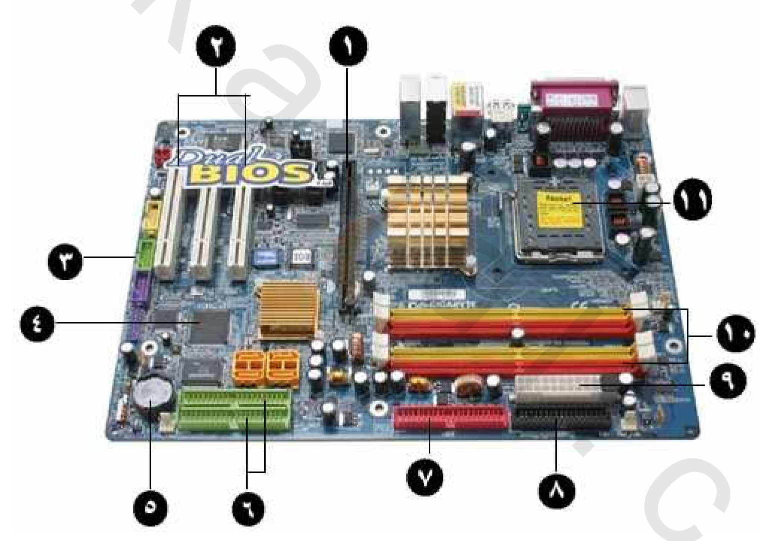
اللوحة الأم:

تعتبر اللوحة الأم (أو اللوحة الرئيسية) **Motherboard** أهم مكونات الكمبيوتر الشخصى على الإطلاق. وقد جاء هذا الاسم من أنها تحتضن كل مكونات الكمبيوتر مثل المعالج والذاكرة والبطاقات ومشغل القرص الصلب والقرص البصرى المختلفة ونظراً لأهميتها الشديدة يجب أن تختار **Motherboard** من النوع الجيد والقابلة للترقية أو

التطوير فيما بعد.

لاشك أن أهم مكونات الكمبيوتر على الإطلاق هى اللوحة الأم أو اللوحة الرئيسية ويطلق عليها مسميات عديدة مثل **Motherboard** أو **Main board** أو **System Board** وكلها تعطى نفس المعنى.

إذا كانت لك خبرة طويلة بالكمبيوتر فإنك ستلاحظ أن اللوحة الأم تتطـور فى شـكلها ومكوناتها تبعاً لتطور الكمبيوترات عموما ومكوناتها الأخرى فقد تطورت ابتداءً مـن أول كمبيوترات شخصية ظهرت بالأسواق فى عام ١٩٨١م باسم **IBM PC** ثم **XT** . فيما يلي صورة للوحة أم حديثة موضح عليها معظم المكونات الأساسية وستجد هـذه المكونـات والمكونات الأخرى بالتفصيل فى الكتيب المرفق مع اللوحة الأم.



شكل اللوحة الأم

١-فتحة توسعة **PCI Express Slot**

٢-فتحات توسعة **PCI slot**.

٣-فتحة توصيل **USB**.

٤-رقيقة القنطرة الجنوبية **(South bridge)**.

٥-البطارية.

٦-

٧-فتحة **IDE**.

٨-موصل محرك القرص المرن.

٩-موصل الطاقة.

١٠-فتحات الذاكرة.

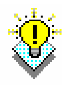
١١-قاعدة توصيل المعالج **(Processor Socket)**

٦–فتحات (IDE ATA Raid).

مكونات اللوحة الأم

تشتمل الأنواع الحديثة من اللوحة الأم على مكونات عديدة فيما يلى أهم هذه المكونات، (بعض الأنواع الحديثة تشتمل على مكونات أخرى مثل وصلة الفيديو والصوت والشبكات).

- قاعدة (مكان) تثبيت المعالج. **Processor Socket / Slot**
- رقائق اللوحة الأم. **Chipset (North/South Bridge or Memory And I/O controller)**
- مكان تثبيت شرائح الذاكرة. **Super I/O Chip**.
- رقائق **I/O**. **ROM BIOS (Flash ROM / Fireware hub)**.
- مكان تثبيت شرائح الذاكرة. **SIMM/DIMM/RIMM (RAM Memory) sockets**
- تجويف (مكان) الكروت التى تثبت على اللوحة. **ISA/PCI/AGP/PCI-EX bus Slots**.
- منظم تيار المعالج. **CPU voltage regulator**.
- البطارية. **Battery**



لمزيد من المعلومات للحصول على معلومات تفصيلية عن هذه المكونات راجع كتابنا "صيانة الحاسبات وتطويرها" أو "تيسير صيانة وتجميع الحاسب".

المعالج Processor

المعالج عبارة عن شريحة من السيلكون المحفور عليها عدة طبقات من أدوات النقل الدقيقة باستخدام عمليات شديدة الدقة والتعقيد.

عادة يتم تركيب المعالج في قاعدة توصيل موجودة على اللوحة الأم (قاعدة التوصيل عبارة عن فتحة في اللوحة الأم تم تصميمها لتوفر عدة وصلات لبعض الأجهزة مثل المعالج والذاكرة والبطاقات المختلفة)

وهو يشبه المخ بالنسبة للإنسان ويشتمل على الدوائر اللازمة لتنفيذ العمليات الداخلية

للكمبيوتر برغم أن طوله لا يتجاوز ٥ سم. ويقوم بمعالجة العمليات الحسابية والمنطقية وهو الذى يتولى تنفيذ تعليمات البرنامج ويعرف ما هو الإجراء الذى يجرى تنفيذه على الكمبيوتر وما هو ترتيبه داخل البرنامج. وهو الذى يوجه المدخلات والمخرجات من وإلى وحدات الإدخال والإخراج الأخرى. وأحيانا يسمى **Microprocessor** بمعنى المعالج الأصغر أو **Central Processing Unit** وتختصر **CPU** ومعناها وحدة المعالجة المركزية.



وحدة المعالج **Processor**

يشتمل المعالج أو وحدة المعالجة المركزية على وحدتين:

الأولى : وحدة الحساب والمنطق **Arithmetic and Logical Unit (ALU)**

وتقوم بأداء العمليات الحسابية مثل: الجمع والطرح والضرب والقسمة أو العمليات المنطقية مثل: مقارنة قيمتين لمعرفة هل هما متساويتين أم أن إحداهما أكبر أو أصغر من الأخرى، واتخاذ القرار المناسب بناء على نتيجة المقارنة. حيث لا تخرج أى عملية من عمليات الكمبيوتر عن هذين النوعين.

الثانية : وحدة التحكم **Control Unit (CU)**

وهى تتحكم فى تدفق البيانات بين أجهزة الكمبيوتر وفى عمليات الإدخال والإخراج. ويمكن تشبيه عملها الذى يتلخص فى تنظيم حركة سير وحدات الكمبيوتر المختلفة بعمل رجل المرور الذى يقوم بتنظيم حركة سير السيارات فى الشارع.

تقاس سرعة المعالج بالميجا هيرتز **(Megahertz)** وتختصر هكذا **MHz** أو بملايين الدورات فى الثانية الواحدة. وكلما زادت سرعة المعالج كلما زادت سرعة تنفيذ العمليات التى يجرى تنفيذها على الكمبيوتر. ويختلف المعالج من كمبيوتر لآخر حسب نوع الجهاز.

وبالتالى تختلف طريقة معالجة البيانات وسرعة تنفيذ البرامج المطلوب تنفيذها على الكمبيوتر تبعا لنوع المعالج وطريقة عمله. ونوضح فيما يلى طريقة عمل المعالج وأنواع المعالجات فى الكمبيوترات الشخصية. ومنه ستعرف التطور الذى حدث لهذا النوع من أجزاء الكمبيوتر.

الذاكرة Memory

ذاكرة الكمبيوتر عبارة عن دوائر الكترونية صغيرة مصنوعة من مادة السيلكون **Silicon** أو أى مادة أخرى شبه موصلة **Semiconductor**. حيث تثبت ذاكرة الكمبيوتر مثلها مثل المعالج على لوحة الكترونية تسمى اللوحة الأم **Mother Board**.

أنواع الذاكرة

يتم تقسيم الذاكرة إلى نوعين أساسيين هما:

أولا : ذاكرة الوصول العشوائي Random Access Memory

النوع الأول يسمى **Random Access Memory** وتختصر هكذا **RAM** أى ذاكرة الوصول العشوائي. وهذه الذاكرة يمكن قراءة محتوياها كما يمكن الكتابة عليها أو حذف محتوياها. لهذا السبب فهي تستخدم لتوضع داخلها البيانات التى يحتاجها المعالج. حينما يحتاج المعالج إلى أى بيانات من وحدات التخزين المثبتة داخل الكمبيوتر، يتم أولاً نقل هذه البيانات من وحدة التخزين إلى الذاكرة ليقوم المعالج بعد ذلك بإجراء العمليات المناسبة على هذه البيانات ثم إرجاعها إلى وحدة التخزين مرة أخرى إذا تطلب الأمر. أى أن الوظيفة الرئيسية للذاكرة **RAM** أها تعمل كوسيط بين المعالج ووحدات التخزين وذلك لاختلاف سرعات كل من المعالج ووحدات التخزين.

ويقاس حجم الذاكرة "بالبايت" **(Byte)**. وهى مكان داخل الذاكرة يسمح بتخزين حرف واحد. ويقال عن كل ١٠٢٤بايت "كيلوبايت" **Kilo Byte** وتختصر هكذا **K.B.** كما يقال عن كل ١٠٢٤كيلوبايت "ميجابايت" (**M.B.**) كما يقال عن كل ١٠٢٤ ميجابايت "جيجابايت" (**G.B.**) فإذا قيل أن هذا الكمبيوتر سعت ذاكرته ١٢٨ ميجابايت، فمعنى هذا أن سعة ذاكرة الوصول العشوائى **RAM** هى ١٢٨ ميجابايت.

ويمكن زيادة حجم الذاكرة المتاحة بإضافة رقــائق جديــدة (**Chips**) إلى اللوحــة الأم (**Mother Board**). ويتم زيادة حجم الذاكرة بمضاعفات الرقم ٦٤ (٦٤ ك.ب.) أى ٦٥٥٣٦ بايت (٦٤×١٠٢٤ بايت) إلا أن هذه الرقائق لها حد معين (لكى تعرف أقصى إمكانية لزيادة كمبيوترك راجع كتيب الشركة الصانعة للوحة الأم).

***ثانيا : ذاكرة القراءة فقط* Read Only Memory**

النوع الثانى يسمى **Read Only Memory** وتختصر هكذا **ROM**. أى ذاكرة القــراءة فقط. وهذه الذاكرة تشتمل على التعليمات اللازمة لتشغيل الكمبيــوتر والــتى تــضعها الشركات الصانعة. أو البرامج الغير مسموح بتعديلها. وهذه البرامج أو التعليمات لا يمكن تعديلها أو حذفها ولكن يمكن قراءتها فقط ولذلك تسمى ذاكرة القراءة فقــط. وهــذه الذاكرة لا يستخدمها المبرمجون أو مستخدمو الكمبيوتر.

الأقراص الصلبة Hard Disks

تتميز هذه الأقراص بالطاقة التخزينية العالية وقصر الزمن اللازم للوصــول إلى البيانــات المخزنة عليها (**Access Time**) وتتميز كذلك بأنها غير قابلة للتبديل أو التغيير أى ثابتة ولذلك تسمى أحيانا الأقراص الثابتة (**Fixed Disks**).

وتتم عملية تسجيل البيانات على هذه الأقراص بنفس الطريقة التى تتم بهــا فى الأقــراص المرنة من حيث أنها تسجل على هيئة نقط مغناطيسية على السطح الممغــنط للقــرص وفى المسارات (**Tracks**). وأيضا يقسم القرص إلى قطاعات تختلف باختلاف طريقة تــشكيل القرص غير أنها تختلف عن الأقراص المرنة فى أنها تصنع من مادة معدنية مغطاة بمادة أكسيد الحديد القابل للمغنطة.

***مشغل القرص الصلب* Hard Disk Drive**

يتكون مشغل القرص الثابت من محور دوران رأسى فى المنتصف يتم وضع مجموعة الأقراص عليه وفوق بعضها وتثبيتها فيه بحيث يكون هناك فراغ بين كل قرص والآخــر للــسماح لأذرع الوصول **Access arms** الحاملة لرؤوس القراءة والكتابة بالدخول بين الأقراص

وملامسة أسطحها المغناطيسية حتى يتمكن الكمبيوتر من قراءة البيانات المخزنة على القرص الثابت من الداخل أو الكتابة علية. ويشتمل الشكل التالي على شكل القرص الصلب من الداخل.



توصيل القرص الصلب بالكمبيوتر

نوضح فيما يلى الطرق المستخدمة لتوصيل القرص الصلب بالكمبيوتر:

الطريقة IDE (اختصار لعبارة **Integrated Drive Electronic**) ويعرف أيضا باسم **ATA** : وهى أرخص الطرق لتوصيل القرص الصلب بالكمبيوتر ويمكن أن يدعم إصدار حديث من **IDE** يطلق عليه **EIDE** أقراص اكبر حجما تصل إلى مئات الجيجابايت ويمكن بها توصيل حتى ٤ أجهزة بالكمبيوتر وتشمل: الأقراص الصلبة وأجهزة تشغيل الأسطوانات المدمجة وأجهزة تشغيل الشرائط.

الطريقة سكازى (SCSI): كلمة **SCSI** اختصار للعبارة **Small Computer System Interface** "واجهة نظام كمبيوتر صغير" وهى طريقة سريعة ومرنة لتوصيل القرص الصلب بالكمبيوتر مع كونها مرتفعة الثمن. ويمكن إن تستخدم لتوصيل أجهزة أخرى بالكمبيوتر مثل جهاز تشغيل الأسطوانات المدمجة وجهاز تشغيل الشرائط والماسحات الضوئية والطابعات وتأتى أجهزة الكمبيوترات عالية الأداء والأجهزة الرئيسية للشبكات مجهزة بنظام التوصيل سكازى.

هناك ثلاثة أنواع للطريقة سكازي:

SCSI-1 : وبها يمكن توصيل حتي ٧ أجهزة بالكمبيوتر في سلسلة (مثلاً ماسح ضوئي أو محرك أشرطة أو طابعة).

SCSI-2 : وبها يمكن توصيل نفس العدد من الأجهزة إلا أنها متوافقة مع أنواع أكثر من الأجهزة الخارجية كما تنقل البيانات بمعدل أسرع وهذه الطريقة هى الطريقة القياسية فى صناعة الكمبيوترات حالياً .

SCSI-3 : وبها يمكن توصيل حتى ١٥ جهاز بالكمبيوتر وتعتبر الأسرع فى معدل نقل البيانات. وعن كل من الطريقتين نقول أن **IDE/ATA** أسهل فى أعدادها وأرخص من أجهزة ومكونات **SCSI**،بينما تعد**SCSI** أسرع وأكثر قابلية للتغيير. إذا كنت تعد جهاز كمبيوتر ليعمل كوحدة خدمة، فان محركات أقراص **SCSI** هى الخيار الأفضل.

فتحات التوسعة Expansion Slots

تحتوي اللوحة الأم علي قواعد توصيل لأجهزة أخري (خلاف المعالج الذي شرحناه) تتعامل مع عدة وظائف من وظائف الكمبيوتر. يطلق علي الأجهزة التي يتم وضعها في قواعد توصيل (فتحات التوسعة) "بطاقات التوسعة" أو "كروت التوسعة" (**Expansion Cards**).سنشرح بطاقات التوسعة بعد قليل.

على الرغم أن معظم اللوحات الأم تشتمل على فتحات توسعة، إلا أن فتحات التوسعة الموجودة على اللوحات الأم ليست متشابهة. حيث تعتمد فتحات التوسعة الموجودة فى اللوحة الأم على كروت التوسعة التى ستركب على اللوحة الأم.

تستخدم هذه الفتحات لنقل البيانات من وإلى الذاكرة ولذلك يطلق عليها ناقلات البيانات لاحظ أنه كلما زادت سرعة نقل البيانات كلما زاد الحصول علي أعلي إمكانيات للكمبيوتر.

تسمي المسارات التي من خلالها تنتقل البيانات من مكان لآخر في الجهاز ناقل أو **Bus** .

بالنسبة لأجهزة الكمبيوتر تعد الناقلات الأكثر شيوعا بترتيب ظهورها من الأقدم إلى الأحدث على النحو التالي

ISA → EISA → PCI

لقد تطورت ناقلات البيانات مع تطور أجهزة الكمبيوتر على النحو التالي :

ISA : ترمز **ISA** إلى العبارة **Industry Standard Architecture** ومعناها "البناء

الصناعي القياسي" ظهر ناقل ISA فى البداية مع كمبيوترات IBM XT فى عام ١٩٨٢ ثم ظهر مع كمبيوترات IBM PC/AT بعد ذلك . لهذا الناقل مساران. الأول يبلغ 8-Bit وهو النوع القديم الذي لم يعد مستخدما. والثاني يبلغ 16 Bit أى أنه يستطيع أن ينقل ١٦"بت" فقط من البيانات فى وقت واحد.

وتبلغ أقصى سرعة نقل بيانات للناقل ISA ٨ ميجا هيرتز .

- EISA : كلمة EISA اختصار للعبارة Extended Industry Standard Architecture . وهذا الناقل وريث ISA ويبلغ عرضه (مسار البيانات) ٣٢بت ، وتصل سرعته إلى ٣٢ ميجا هيرتز .
- Local Bus : يقوم هذا الناقل بحل مشكلة بطء ناقلات المدخلات والمخرجات (ISA، EISA) بالمقارنة لسرعات ناقلات الذاكرة والمعالج .
- VL–BUS : (VESA Local Bus) وهو تعديل للناقل الذي سبقه وكان اسمه Local Bus. ويوفر للذاكرة سرعة تماثل سرعة المعالج حيث يمكن نقل 32-bits، وتصل سرعته إلى ١٢٨–١٣٢ ميجا هيرتز.

أصبحت الأنواع السابقة من الناقلات ISA و EISA و Local Bus و VL–BUS تكنولوجيا قديمة ولا يعرفها إلا الجيل السابق مثلى. معظم مستخدمي الكمبيوترات الحديثة لم يروا هذه الناقلات ولم يعرفوها .

- PCI : كلمة PCI اختصار للعبارة Peripheral Component Interconnect BUS ويمكن ترجمتها(توصيل داخلي للمكونات الطرفية) وهى تعديل للناقل ISA و EISA وظهر في أوائل التسعينات ويتسم PCI بسرعة هائلة حيث تصل سرعة نقل البيانات بواسطته إلى ١٢٨ميجا بايت فى الثانية فى المعالجات 32–bit، وبالطبع عند استخدام معالجات 64–bit فان معدل نقل البيانات سيتضاعف ويصل إلى ٢٦٤ ميجا بايت فى الثانية.

بطاقات التوسعة Expansion Cards

بطاقات التوسعة Expansion Card عبارة عن لوحة الكترونية تثبت فى فتحة التوسعة

(غالبا تأتى الكمبيوترات وبها الكثير من بطاقات التوسعة).

تركب كروت التوسعة في فتحات أو شـقوق موجـودة علـى اللوحـة الإم تـسمى Expansion Slots "فتحات توسعة". وكلما زادت فتحات التوسعة على اللوحة الام كلما أمكنك إضافة مميزات جديدة له. ومن أمثلة بطاقات التوسعة بطاقة الشبكة وبطاقـة الفيديو .

فيما يلي نلقى بعض الضوء على أهم بطاقات التوسعة و نخص بالشرح تلك التي ستتعامل معها مثل بطاقة الشبكة و بطاقة الفيديو وبطاقات SCSI.

***بطاقات الشبكة* Network Adapter Card**

تسمح بطاقة الشبكة (Network Adapter Card) بتبادل البيانات بين الكمبيـوترات المرتبطة مع بعضها داخل شبكة اتصالات

تسمى بطاقة الشبكة أحيانا Network Interface Card وتختصر هكذا NIC، ومعناها " بطاقة واجهة استخدام الشبكة ".

تأتى معظم أجهزة الكمبيوتر اليوم مركب عليها بطاقة شبكة إذا لم يكن الكمبيوتر مشتملا على بطاقة شبكة. يجب إن تقوم بنفسك بتركيبها .

من الأمور التي يجب إن تعرفها وتتذكرها عن بطاقة الشبكة انه يتم تعيين رقم فريد مكون من ٤٨ بت (أى٦بايت) لكل بطاقة. ويطلق على هذا الـرقم عنـوان MAC (Media Access Control).

***بطاقة الفيديو* Video Adapter Card**

بطاقة الفيديو هي المسئولة عن ظهور الصورة على الشاشة. تأخذ بطاقة الفيديو البيانـات الرقمية التي يستخدمها جهاز الكمبيوتر داخليا وتحولها إلى تنسيق قياس أو شـكل موجـه يمكن عرضه على شاشة الكمبيوتر.

يطلق على ادني مقياس لشاشات عرض الفيديو على أجهزة الكمبيوتر الحديثة اسم VGA (Video Graphic Array). ويطلق على بطاقة الفيديو أحيانا بطاقة VGA .

لم تعد VGA تلبى طموحات المستخدمين، حيث تعرض الصورة على الشاشة بعدد٦٤٠

بكسل عرضا في٤٨٠ بكسل طولا، بستة عشر لونا على الأقل. وهو ما لا يمكنها من عرض الصور والألوان بدقة شديدة. دفع هذا الوضع الشركات إلى تطوير بطاقات فيديو تجعل الصورة أدق وأوضح أطلق علي **Super VGA** . يمكنها إن تعرض عدد ٨٠٠ بكسل عرضاً X٦٠٠بكسل طولا في ١٦لون. ثم طورت الشركات بطاقة **Extended VGA** (تبلغ ١٠٢٤ بكسل عرضا في ٧٦٨ بكسل طولا)

تقدم إعدادات العرض الإضافية لبعض البطاقات عدد ألوان على الشاشة يتراوح بين ٢٥٦ إلى ١٦,٧ مليون لون. وهى جودة عالية تضاهى الصور الفوتوغرافية.

ثانيا: البرامج (Soft ware)

كلمة "سوفت وير" (**Software**) تستخدم للدلالة علي البرنامج الذي يقوم بوظيفة محددة. وهذه البرامج يقوم بكتابتها أشخاص مدربون. وتباع بمحلات بيع الكمبيوترات مثل أشرطة الكاسيت. ويمكننا أن نقول أن البرامج (**Software**) هي التي تشغل الأجهزة (**Hardware**). فالجهاز بدون برامج يشبه السيارة بدون بنزين فبدون البرامج فإن الكمبيوتر لا يعدو كونه قطعة ديكور أو آلة غير ذات جدوى. إذا كان الكمبيوتر لا يفهم ولا يضع خططا ولا يحل مشاكل بمفرده فإن البرنامج هو الذي يوجه الكمبيوتر لحل المشاكل ووضع الخطط المناسبة. ويتكون البرنامج من مجموعة من التعليمات تحدد العمليات المطلوب تنفيذها وترتيب تنفيذها علي الكمبيوتر . فالبرنامج الواحد قد يشتمل علي مئات بل آلاف التعليمات . ويوضع البرنامج أثناء التنفيذ داخل ذاكرة الكمبيوتر. ويقوم بكتابة البرنامج شخص مدرب بسمي المبرمج (**Programmer**) وبعد الانتهاء من كتابة البرنامج وتجربته يمكن تنفيذه علي الكمبيوتر لعدد غير محدود من المرات . ويمكن حفظه علي أحد وسائط التخزين المعروفة مثل الأقراص المغناطيسية. تنقسم البرامج التي يمكن تشغيلها علي الكمبيوتر إلي نوعين رئيسيين علي النحو التالي :

برامج نظم التشغيل وتسمي **Operating Systems Programs**

وهي البرامج التي تتحكم في سير العمل علي الكمبيوتر وفي تنفيذ البرامج الأخرى . بعبارة أخري برامج النظم هي التي تساعد الكمبيوتر علي إدارة نفسه وخلق وسيلة اتصال بيننا

وبينه ومن أمثلتها نظام التشغيل **Windows** ونظـــام **Unix** ســـنعود لـــشرح نظـــم **Windows** و**Unix** لأهميتها وحاجتنا إليها في هذا الكتاب.

البرامج التطبيقية وتسمي Application Programs

وهي برامج تخدم الهدف الذي كتبت من أجله. أي أنها البرامج التي تقوم بتنفيذ أعمالنـــا المختلفة. ومن أمثلتها برنامج حساب مرتبات العاملين بالمؤسسة. وإلى هذا النوع تنتمـــي الحزم البرمجية الجاهزة وتسمي **Ready Package** ومن أمثلتها :

- برامج معالجة النصوص(**Word Processing Software**)
- برامج قواعد البيانات(**Data Base Software**)
- برامج الرسوم (**Graphics Software**)
- برامج العروض (**Presentation**)
- برامج الجداول الحسابية (**Spreadsheet**)

ملخص الفصل

شرحنا فى هذا الفصل مكونات الكمبيوتر الأساسية وقسمناها إلى مكونات مادية وبرامج ثم شرحنا المكونات المادية للكمبيوتر لكى تفهم فيما بعد مكونات الشبكة. وختمنا الفـــصل بتوضيح أهم برامج نظم التشغيل وبرامج التطبيقات.

تدريبات

١. تسمى الفتحات التي تنقل البيانات بين بطاقات التوسعة ووحدة المعالجـــة المركزيـــة (فتحات التوسعة / كروت الشبكة / وسائط التخزين).

٢. رتب ناقلات البيانات (فتحات التوسعة) الآتية من الأقدم إلى الأحدث:

أ. **PCI**

ب. **ISA**

ج. **ELSA**

٣. أي من المنافذ التالية يصنف كمخارج فقط للنظام:

أ. منفذ الطابعة

ب. منفذ الفارة

ج. منفذ لوحة المفاتيح

د. منفذ بطاقة الشاشة

٤. اختر الإجابة الصحيحة:

أ. تسمى المنافذ المتوالية **Serial Ports** بالاسم **COM** مضافاً إليه رقم للتميز

ب. تسمى المنافذ المتوازية **Parallel Ports** بالاسم **LPT** مضافاً إليه رقم التميز

ج. المنافذ المتوازية أسرع من نظيرتها على التوالي

د. كل ما سبق

هـ. لا شئ مما سبق في نفق البيانات

٥. اختر الإجابة الصحيحة:

أ. الذاكرة **RAM** محتوياتها (ثابتة / متغيرة)

ب. القرص الصلب (أسرع / أبطأ) من القرص المرن

ج. تسمى البرامج التي تتحكم في سير العمل على الكمبيوتر وفي تنفيذ البرامج الأخرى (برامج تطبيعية / برامج نظم التشغيل)

د. أشهر بطاقة توسعة تستخدم مع الشبكات تسمى (بطاقة الصوت / بطاقة الفيديو / بطاقة الشبكة)

٦. اذكر أربعة من أشهر البرامج التطبيقية

٧. أهم المكونات التي تتحكم في سرعة الكمبيوتر:

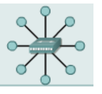
أ. الذاكرة

ب. المعالج

ج. سرعة القرص الصلب

د. كل ما سبق

هـ. لا شئ مما سبق





*شرحنا في الفصل السابق مكونات الكمبيوتر وقسمناها إلي مكونات مادية **Hardware** وبرامج **Software** وفي هذا الفصل نشرح مفاهيم تهم العاملين في مجال الشبكات .*

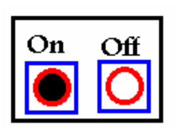
بانتهاء هذا الفصل ستتعرف علي :

- *تمثيل الأرقام والحروف والرموز باستخدام شفرة **ASCII**.*
- *كيف يتم تخزين البيانات داخل الذاكرة.*
- *نظم الأعداد.*
- *حساب سرعة نقل البيانات.*

كيف يتم تخزين البيانات داخل الذاكرة

يحتل الحرف الواحد أو الرقم أو الرمز (نقصد بالرمز هنا أى مفتاح بلوحة المفاتيح عدا الحروف الأبجدية والأرقام من صفر إلى تسعة ومن أمثلتها هذه الرموز: . و "؛ $ + = – * !) مساحة قدرها ١ بايت (Byte) داخل ذاكرة الكمبيوتر. و لكن هل يفهم الكمبيوتر الحروف والأرقام والعلامات؟ بعبارة أخرى هل يستطيع الكمبيوتر التفرقة بين الحرف A والحرف Z . أو بين الرقم ٧ وعلامة الجمع +. . . ؟ للأسف لا. إذن كيف يتعرف الكمبيوتر على الحروف والرموز؟. للإجابة على هذا السؤال لابد أن تفهم كيف يتم تخزين البيانات داخل ذاكرة الكمبيوتر.

قلنا أن الذاكرة تتكون من العديد من الدوائر الكترونية. وتستطيع هذه الدوائر أن تستشعر مرور التيار الكهربائى داخلها من عدمه. ولذلك فإن أصغر وحدة لتخزين البيانات داخل الذاكرة ليست "البايت". وإنما هى "البت" (Bit) (مأخوذة من كلمة (Binary Digit) وتشتمل كل "بت" Bit داخل الذاكرة على إحدى قيمتين : صفر (0) أو واحد (1). وتمثل "البت" التى تشتمل على الرقم 0 دائرة مفتوحة أى أن التيار الكهربائى لا يمر داخلها. بينما تمثل "البت" التى تشتمل على الرقم 1 دائرة مغلقة أى أن التيار الكهربائى يمر داخلها. ويقال عن البت التى تحتوى على الرقم 0 فى حالة OFF بينما يقال عن "البت" التى تحتوى على الرقم 1 فى حالة ON. (انظر شكل ٣– ١).



شكل ٣–١ تشير الدائرة السوداء على أن الدائرة مغلقة ، أى أنها فى حالة OFF
بينما تشير الدائرة البيضاء إلى أن الدائرة مفتوحة أى أنها فى حالة ON

ولا يمكن تخزين حرف أو رقم أو رمز داخل "البت" الواحدة. وبدون تخزين الحروف الأبجدية أو الأرقام أو الرموز داخل الذاكرة لا تتحقق الاستفادة من الكمبيوتر ولذلك لجأ مصمموا الكمبيوتر إلى استخدام أكثر من "بت" bit متجاورة لتخزين الحرف الواحد أو الرقم الواحد أو الرمز الواحد. وتستخدم معظم الكمبيوترات كل ٨ "بتس" متجاورة

لتخزين الحرف أو الرقم أو الرمز. وتسمى كل ٨ "بتس" متجاورة "بايت" **Byte**. وعلى هذا فإن كل "بايت" عبارة عن مكان داخل الذاكرة يتكون من ٨ "بتس" متجاورة (انظر شكل ٣–٢).

8 - BIT BYTE

شكل ٣–٢ كل ٨ **BITS** داخل **BYTE** تستخـــدم لتخـــزين حـــرف أو رقـــم أو رمـــز ويخصص لكل حرف أو رقم توليفة بعضها فى حالة**ON** والبعض الآخر فى حالة **OFF** بحيث لا تتشابه مع توليفة حرف آخر.

الشفرة ا لأمريكية القياسية لتبادل المعلومات ASCII

تستخدم معظم الكمبيوترات الصغيرة الشفرة الأمريكية القياسية لتبادل المعلومات لتمثيل البيانات داخل الذاكرة وتعرف بهـــذه العبـــارة **American Standard Code for Information Interchange** وتختصر هكذا **ASCII** وتنطق "آسكى".

باستخدام شفرة **ASCII** يتم تخزين كل حرف أو رمز أو رقم على حدة داخـــل "بايـــت" واحدة. فمثلا الرقم ٩٥١ يحتاج لمساحة قدرها ٣ "بايت" من الذاكرة. ولكى تأخذ الأرقام داخل الذاكرة معنى حقيقيا يخصص لكل "بت" داخل "البايت" قيمة بناء على ترتيبها داخل البايت من اليمين إلى اليسار. وتعتمد القيمة المخصصة لكل "بت" داخل "البايت" علـــى النظام الثنائى **(Binary System)**. (سوف نشرح بعد قليل النظام الثنائي ضمن نظـــم الأعداد)

تمثيل الأرقام والحروف والرموز باستخدام شفرة ASCII

سنشرح فيما يلي كيفية تمثيل الأرقام والحروف والرموز داخل ذاكرة الكمبيوتر باستخدام الشفرة الأمريكية القياسية لتبادل المعلومات والمعروفة اختصاراً بـــــ **ASCII**.

يتم تمثيل الأرقام العشرية باستخدام شفرة **ASCII** على النحو التالي:

- "البتس" الأربعة الموجودة على يمين "البايت" (من **0** إلى **3**) تستخدم لتمثيل الأرقـــام العشرية من صفر إلى تسعة. ذلك بوضع "البت" أو "البتس" التى تقابل الرقم المطلوب

فى حالة **ON**.

- "البتس" رقم ٤و٥ دائما فى حالة **ON**.
- "البتس" رقم ٦و٧ دائما فى حالة **OFF**.

وللتوضيح نسوق المثال التالى:

لتمثيل الرقم 4 داخل "البايت" يجب أن تكون "البتس" الثمانية على النحو التالى:

- توضع "البت" رقم ٢ فى حالة **ON**. ومعناها فى هذه الحالة أثنين أس أثنين أى أربعة.
- توضع "البت" رقم ٤و٥ فى حالة **ON** لأنها كما قلنا دائما فى حالة **ON**.
- توضع "البت" الباقية فى حالة **OFF**.

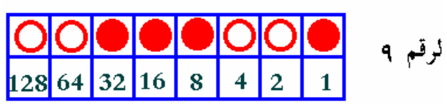
وبهذا يظهر الرقم ٤ داخل الكمبيوتر بالنظام الثنائى هكذا **00110100**. وبنفس الطريقة يمكن تمثيل الرقم ٩ على النحو التالى:

- توضع كل من "البت" رقم صفر ورقم ٤ فى حالة **ON** (لاحظ أن "البت" رقم صفر معناها أثنين أس صفر أى واحد و"البت" رقم ٤ معناها أثنين أس ثلاثة أى ثمانية. وبجمع ١+٨ يكون المجموع ٩.
- توضع كل من "البت" رقم أربعة و خمسة فى حالة **ON**.
- توضع باقى "البت" فى حالة **OFF**.

وبهذا يظهر الرقم ٩ داخل الكمبيوتر بالنظام الثنائى هكذا:**00111001**. (انظر شكل ٣-٣) ومنه تلاحظ أن البتس ٥،٦ فى الرقمين فى الوضع **ON** وأن البتس المقابلة للرقم المطلوب من الأربعة الأولى أيضا فى وضع **ON**.

الرقم ٤

128 64 32 16 8 4 2 1



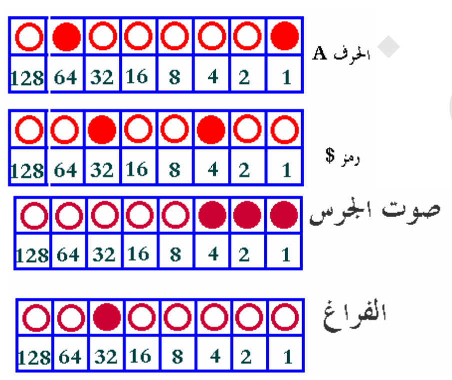
شكل ٣-٣ يتم تمثيل الأرقام باستخدام شفرة **ASCII** بوضع "البتس" رقم ٥ و ٦ دائماً فى حالة **ON** ووضع "البتس" المقابلة للرقم المطلوب من الأربعة الأولى كذلك فى حالة **ON**.

تذكر أننا قلنا أن الرقم الواحد (من صفر إلى تسعة) يحتاج بايت كاملة داخل الذاكرة. فإذا أردت مثلا تخزين الرقم ٤٥ فيلزمك فى هذه الحالة أثنين "بايت" متجاورين.

تمثيل الحروف والرموز باستخدام شفرة "اسكى"

يخصص لكل حرف أو رمز من الحروف الهجائية أو الرموز كود معين يتم الحصول عليه بوضع توليفة مختلفة من "البتس" فى حالة **ON** أو **OFF** بحيث لا تتشابه مع توليفة أخرى مخصصة لحرف أو رمز آخر. فمثلا الحرف **A** يتم تمثيله داخل "البايت" هكذا : **01000001**. ولما كانت الصفر تعنى أن البت فى حالة **OFF** والواحد تعنى أن البت فى حالة **ON**. معنى هذا أن البت داخل البايت من اليمين إلى اليسار بالترتيب التالى : **OFF ON OFF OFF OFF OFF OFF ON** . كما تمثل علامة الدولار ($) داخل البايت هكذا : **00100100**. وهذا يعنى أن البتس رقم ٧،٦،٤،٣،١،٠ فى حالة **OFF** أما البتس رقم ٢ ، ٥ ففى حالة **OFF**.

ونود أن نوضح هنا أمرا هاما وهو أن العلامات والرموز التى لا تظهر على لوحة المفاتيح والتى تستخدم بواسطة الكمبيوتر لأداء وظيفة معينة تمثل بنفس الطريقة. فمثلا يوجد كود للفراغ وكود لصوت الجرس الذى يسمع أحيانا لتنبيه المستخدم أو فى برامج الألعاب. ويوضح الشكل التالي كيفية تمثيل الحروف والرموز التى أشرنا إليها. وبنفس الطريقة تستطيع أن تفهم باقى الحروف والرموز التى يستخدمها الكمبيوتر. (انظر شكل ٣–٤)



شكل ٣–٤ يتم تمثيل الحروف الأبجدية والرموز والعلامات الخاصة داخل الذاكرة باستخدام شفرة **ASCII** بوضع توليفة من "البت" لكل حرف فى حالة **ON** أو **OFF** بحيث تختلف عن الأخرى

نظم الأعداد

نشرح في هذا الفصل ثلاثة أنواع من نظم الأعداد ونوضح كيف يمكن التحويل من نظام إلي آخر . نظم الأعداد التي سنتناولها هنا هي :

- النظام العشري Decimal System
- النظام الثنائي Binary System
- النظام السداسي عشر Hexadecimal System

أولاً : النظام العشري Decimal System

النظام العشري هو نظام الأعداد المألوف لنا من دراستنا لعلم الحساب فى المراحل الأولية من التعليم والذي يعتمد على الأساس عشرة لأن أعداده عددها عشرة وهى:٩،٨،٧،٦،٥،٤،٣،٢،١،٠ وتذكر معى أن الرقم ٩٩٩ فى النظام العشرى يتكون من ثلاثة أعداد : الأول فى خانة الآحاد والثانى فى خانة العشرات والثالث فى خانة المئات. ولذلك فإن التسعة الموجودة فى أقصى اليمين معناها تسعة فى عشرة أس صفر (٩×١٠^{٠}) أى تسعة فى واحد أى تسعة. والتسعة التى تليها معناها تسعة فى عشرة أس واحد (٩×١٠^{١}) أي تسعون. أما التسعة الأخيرة فمعناها تسعة فى عشرة أس أثنين (٩×١٠^{٢}) أى تسعمائة. وينطق الرقم تسعمائة وتسعة وتسعون (انظر شكل٣– ٥). ورغم أن هذا المثال واضح لنا جميعا إلا أنني قصدت من ورائه إلى توضيح فكرة النظام الثنائي الغير معروف بمقارنته بالنظام العشري المعروف.

الرقم العشري	٩	٩	٩
القيمة المكانية للعدد	آحاد	عشرات	مئات
القوة	١٠ صفر	$١٠^{١}$	$١٠^{٢}$

شكل ٣–٥ يتم الحصول على الرقم ٩٩٩ فى النظام العشري المعروف بتخصيص قيمة لكل خانة حسب ترتيبها داخل الرقم.

ثانياً : النظام الثنائى Binary System

النظام الثنائى (Binary System) نظام الأساس فيه اثنين لأنه يشتمل على عددين فقط هما صفر وواحد. وفى النظام الثنائى تأخذ "البتس" داخل البايت القيم التالية

من اليمين إلى اليسار ١-٢-٤-٨-١٦-٣٢-٦٤-١٢٨. وترقم "البت" داخل "البايت" من صفر إلى سبعة ويخصص "للبت" الموجودة فى أقصى اليمين الرقم صفر. والتى تليها الرقم واحد. . . وهكذا حتى تصل إلى "البت" الموجودة فى أقصى اليسار فيكون رقمها هو سبعة. (انظر شكل٣-٦) .

7	6	5	4	3	2	1	0	رقم البت الببتس قد تكون
O	O	O	O	O	O	O	O	فى حالة ON أو OFF
128	64	32	16	8	4	2	1	القيمة المكانية للعدد

شكل ٣-٦ كل "بت" داخل "البايت" قيمة تستمد من ترتيبها داخل "البايت" تبعاً للنظام الثنائي الذى يعتمد على الأساس ٢.

النظام الثنائي يتكون من رمزين اثنين هما صفر (**0**) و واحد (**1**) ولذلك فأن النظام الثنائي نظام الأساس فيه ٢ وليس ١٠ لأن عدد رموزه ٢ فقط ولشرح فكرة الصفر والواحد نقول أن الكمبيوتر يتكون من دوائر الكترونية . هذه الدوائر يمكن أن يمر بها تيار كهربي أو لا يمر. الدائرة التى يمر بها تيار كهربى تكون مغلقه يعنى بها رقم **1** والدائرة التي لا يمر بها تيار كهربي تكون مفتوحة يعني بها صفر . وتسمي كل منها **bit** (بت) . ويتم تمثيل كل حرف من حروف الهجاء أو رقم أو رمز يستخدم في الكتابة داخل ذاكرة الكمبيوتر بثمانية بتات (**8 Bits**) وتسمي هذه البتات الثمانية بايت (**Byte**)

التحويل من النظام الثنائي إلي النظام العشري

للتحويل من النظام الثنائي إلي النظام العشري نضرب الرمز في قوي ٢ التي تتناسب مع مواقع هذه الرموز ثم نجمع الكل

انظر المثال التالي :

110101

$$2^5 \times 1 + 2^4 \times 1 + 2^3 \times 0 + 2^2 \times 1 + 2^1 \times 0 + 2^0 \times 1 =$$

$$32 + 16 + 0 + 4 + 0 + 1 = 53$$

إذن الرقم الثنائي **110101** = الرقم العشري **53**

التحويل من النظام العشري إلي النظام الثنائي

في المثال السابق للتحويل من النظام الثنائي إلي النظام العشري كنا نكرر عملية الضرب في الأساس ٢ . للتحويل من النظام العشري إلي النظام الثنائي يجب أن تكرر عملية القسمة علي ٢ . ولأننا نقسم علي ٢ فإن الباقي إما أن يكون صفراً (إذا كان العدد زوجي) أو " واحد " إذا كان العدد فردي . وبوضع سلسلة الرموز من الاصفار والآحاد بجانب بعضها يتكون لدينا الرقم الثنائي المكافئ للرقم العشري .

مثال : لتحويل الرقم 53 الذي شرحناه في المثال السابق من النظام العشري إلي النظام الثنائي تابع الخطوات الآتية .

١. اقسم الرقم 53 علي 2 تحصل علي الناتج 26 وباقي القسمة هو 1
٢. اقسم الناتج من الخطوة رقم ١ وهو 26 علي 2 تحصل علي الناتج 13 وباقي قسمة هو 0
٣. اقسم 13 علي 2 تحصل علي الناتج 6 وباقي قسمة هو 1
٤. اقسم 6 علي 2 تحصل علي ناتج 3 وباقي قسمة هو 0
٥. اقسم 3 علي 2 تحصل علي ناتج 1 وباقي قسمة هو 1
٦. اقسم 1 علي 2 تحصل علي ناتج 0 وباقي قسمة هو 1
٧. اكتب البواقي التي حصلت عليها مبتدءاً بآخر باقٍ ومنتهياً بأول باقٍ حصلت عليه .

ستحصل علي العدد الثنائي التالي 110101

فيما يلي طريقة أخري تساعدك في التحويل من النظام العشري إلي النظام الثنائي .

رقم الخطوة	المقسوم	المقسوم عليه	ناتج القسمة	الباقي
1	53	2	26	1
2	26	2	13	0
3	13	2	6	1
4	6	2	3	0
5	3	2	1	1
6	1	2	0	1

ثالثاً : النظام السداسي عشر (Hexa decimal)

يتكون النظام السداسي عشر من ستة عشر رمزاً (في مقابل رمزين للنظام الثنائي

وعشرة رموز للنظام العشري وهذه الرموز هي :

0 – 1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 – 9 – A – B – C – D – E – F

ولكي تتذكر هذه الرموز تذكر أن الرموز من 0 إلي 9 المستخدمة في النظام العـــشري يضاف بعدها الحروف الأبجدية A مقابل 10 و B مقابل 11 ، C مقابل 12 ، D مقابل 13 ، E مقابل 14 ، F مقابل 15

التحويل من السداسي عشر (Hex) إلي العشري (Dec)

لأن النظام السداسي عشر يتكون من ١٦ رمزاً فإن الأساس فيـــه هـــو ١٦ . تستخدم نفس المفاهيم التي شرحناها في النظام العشري والنظـــام الثنـــائي مـــع النظـــام السداسي عشر . مع استبدال استخدام الأساس ١٦ بدلاً من الأساس ١٠ أو الأساس ٢. انظر المثال التالي

لتحويل الرقم السداسي عشر 3D7B إلي رقم عشري

$3 \times 16^3 + D \times 16^2 + 7 \times 16^1 + B \times 16^0 =$

$3 \times 16^3 + 13 \times 16^2 + 7 \times 16^1 + 11 \times 16^0 =$

$12288 + 3328 + 112 + 11 = 15739$

التحويل من العشري (Dec) إلي السداسي عشر (Hex)

في المثال السابق أي للتحويل من السداسي عشر إلي النظام العشري كنا نكـــرر عملية الضرب لرموز العدد بإحدى قوي الأساس ١٦. أما في التحويل من العـــشري إلي السداسي عشر فإننا نقوم بعملية عكسية. يعني نقسم العدد علي ١٦. عندما نقسم الرقم علي ١٦ نحصل علي ناتج وباقٍ . الباقي يجب أن يكون أحد الرموز الست عشرة المكونة للنظام السداسي عشر . يجب أن تكرر عملية القسمة حتي تحصل علي ناتج يساوي صفراً وباقٍ يحتوي علي أحد الرموز الستة عشر .

بعد انتهاء عملية القسمة يكون مجموعة البواقي التي حصلنا عليها هي القيمـــة الـــست عشرية المكافئة للرقم العشري . ابدأ بوضع آخر باق حصلت عليه في أخـــر خطـــوة في أقصي اليسار حتي تصل إلي أول باق في أقصي اليمين .

مثال : لتحويل الرقم العشري السابق وهو 15739 إلي رقم سداسي عشر اتبع الآتي :

١. ابدأ بقسمة الرقم 15739 علي 16 تحصل علي ناتج قسمة يساوي 983 وباق قيمته 11
٢. اقسم 983 علي 16 تحصل علي ناتج يساوي 61 وباق قيمته 7
٣. اقسم 61 علي 16 تحصل علي ناتج يساوي 3 وباقٍ قيمته 13
٤. اقسم 13 علي 16 تحصل علي ناتج يساوي 0 وباقٍ قيمته 3
٥. ضع البواقي التي حصلت عليها بجانب بعضها ابتداءً من آخر باقٍ في اقصي اليسار إلي أول باقٍ في أقصي اليمين هكذا

3 13 7 11

وهي تساوي 3 D 7 B

التحويل من النظام السداسي عشر (Hex) إلي النظام الثنائي (Binary)

رغم أنه بإمكانك تحويل النظام السداسي عشر إلي نظام عشري ثم تحويل النظام العشري إلي النظام الثنائي ، إلا أن الطريقة المثلي والمتبعة في التحويل من النظام السداسي عشر إلي النظام الثنائي هي تمثيل كل رمز في السداسي عشر بأربعة رموز ثنائية . وذلك لأن أكبر رمز في السداسي عشر هو F وهي تساوي بالنظام العشري 15 وبالنظام الثنائي 1111. ونوضحها كما يلي :

$1 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 =$
$8 + 4 + 2 + 1 = 15$

وأقل قيمة هي 0 وبالنظام الثنائي 0000

$0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 0 \times 2^0 =$
$0 + 0 + 0 + 0 = 0$

يوضح الجدول التالي الرموز الست عشرية ومكافئتها من العشرية

العشري	الثنائي	السداسي عشر
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6

العشري	الثنائي	السداسي عشر
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

التحويل من النظام الثنائي (Binary) إلي النظام السداسي عشر (Hex)

تحتاج عملية التحويل من النظام الثنائي إلي النظام السداسي عشر إلي التفكير قليلاً . سنستخدم الجدول السابق لمساعدتنا في التفكير هنا . من الجدول تلاحظ أن اكبر رقم في النظام السداسي عشر يقابله أربع آحاد في النظام الثنائي . لهذا سنستخدم هذا المفهوم في التحويل من الثنائي إلي العشري .

قسم الرقم الثنائي إلي مجموعات . كل مجموعة تتكون من أربع رموز ثنائية وعند تحويل الرموز الأربعة الثنائية سيقابلها قطعاً رمزاً سداسي عشر

ابدأ تقسيم الرموز الثنائية من اليمين حتي تصل إلي أقصي اليسار . إذا لم تشتمل المجموعة الأخيرة علي أربع رموز أكمل البتات المتبقية بأصفار ليكون مجموع رموزها أربعة . بعد تقسيم كل الرقم إلي مجموعات كل منها أربعة رموز ، حول كل مجموعة برمز واحد سداسي عشر. عندما تنتهي من تحويل كل مجموعة (٤ بتات) إلي المقابل الست عشري تكون قد حولت الرقم الثنائي إلي رقم سداسي عشر .

مثال : انظر الرقم الثنائي 11110101111011

لتحويله إلي رقم سداسي عشر اتبع الآتي

١. قسم الرقم إلي مجموعات كل منها ٤ بتات مبتدئاً من اليمين هكذا

0011 1101 0111 1011

٢. حول كل مجموعة إلي رقم سداسي عشري هكذا

3 D 7 B

حساب سرعة نقل البيانات

قياس حجم البيانات

من المعلوم أن الكمبيوتر لا يفهم اللغة التي يتعامل بها البشر في القراءة والكتابة . لابد أن تتحول البيانات التي يقوم الكمبيوتر بمعالجتها إلي سلسلة من الأصفار والآحاد يعني أن الكمبيوتر يحول الأرقام والحروف إلي النظام الثنائي وهو 0 أو 1 وبعد معالجة البيانات يحولها مرة أخري إلي لغة نفهمها نحن عنه .

يستخدم الكمبيوتر شفرة معينة لتحويل الحروف والأرقام إلي رموز 0 أو 1 . تسمي هذه الشفرة ASCII وتنطق هكذا "اسكي" ويتم تمثيل البيانات داخل ذاكرة الكمبيوتر برموز ثنائية (صفر أو واحد) .

باستخدام شفرة ASCII يتم تخزين كل رقم أو حرف أو رمز علي حده داخل بايت (Byte) واحدة فمثلاً الرقم 951 يحتاج لمساحة قدرها ٣ "بايت" من الذاكرة وتتكون كل "بايت" من ٨ "بت" (Bits)

ويقال عن كل ١٠٢٤ بايت " كيلو بايت" Kilo Byte وتختصر هكذا .K.B كما يقال عن كل ١٠٢٤ كيلو بايت "ميجا بايت" (.M.B) كما يقال عن كل ١٠٢٤ ميجا بايت "جيجا بايت" (.G.B)

يوضح الجدول التالي بعض وحدات قياس الذاكرة وبالتالي قياس حجم البيانات .

الوحدة	حجمها	تعرف بـــ
بت Bit	رمز ثنائي 0 أو 1	1 Bit
بايت Byte	8 Bits	1 Byte
كيلو بايت (K.B.) Kilo Byte	1024 Byte	1000 Byte
ميجا بايت (M.B) Mega Byte	1024 K.B.	1 Million Byte
جيجا بايت (G.B.) Giga Byte	1024 M.B.	1 Billion Byte

الوحدة	حجمها	تعرف بـــــ
تـــــيرا بايــــــت (T.B.) Tera Byte	1024 G.B.	1 Trillion Byte

تردد النطاق (**Bandwidth**)

Bandwidth (تردد النطاق) هو قيمة لقياس قدر البيانات التي يمكن لوســط معين حملها . أي عدد من البتات المرسلة أو المستقبلة في الثانيــة الواحــدة **Bits Per Second (bps)** . علي سبيل المثال يبلغ تردد النطاق لخط الهاتف المتوسط نحــو **33.6** كيلو بت في الثانية فقط ، بينما يبلغ تردد النطاق لخط هاتف رقمي **T1** نحو **1.544** ميجا بت في الثانية

ونوضح فيما يلي وحدات تردد النطاق المستخدمة لقياس كمية المعلومــات المرســلة او المستقبلة خلال فترة معينة من الزمن (تقاس عادة بالثانية) .

وحدة القياس	كمية المعلومات
بت في الثانية **Bit per Second**	بت واحدة في الثانية
كيلــو بــت في الثانيــة **Kilo bits per Second**	**1 Kbps = 1000 bps**
ميجا بت في الثانيــة **Mega bits per Second**	**1 Mbps = 1000,000 bps**
جيجا بــت في الثانيــة **Giga bits per Second**	**1 Gbps = 1000,000,000 bps**

تختلف سرعة نقل البيانات حسب نوع الوسط الذي يستخدم لإرسال واستقبال البيانات فبينما تبلغ في خط الهاتف العادي نحو **33.6** كيلو بت في الثانية ، تبلغ في خــط الهــاتف الرقمي **T1** نحو **1.544** ميجابت في الثانية . أيضاً بينما تصل سرعة نقل البيانات عبر بطاقة الشبكة إلي **1000 Mbps** ، قد تكون هذه السرعة مــا بــين **33 Kbps** و **56 Kbps** بالنسبة لجهاز المودم .

نوضح فيما يلي بعض سرعات نقل البيانات عبر وسائط مختلفة .

نوع الوسيط	تردد النطاق (bandwidth)
Modem	56 Kbps
ISDN	128 Kbps
خط T1	1.544 Mbps
خط T3	44.736 Mbps
E1	2.048 Mbps
E3	34.368 Mbps
STS – 1 (OC – 1)	51.840 Mbps
STS – 3 (OC – 3)	155.251 Mbps
STS – 48 (OC – 48)	2.488320 Gbps

من خلال هذا الجدول نستطيع أن نحسب الزمن الذي سيستغرقه ملف ذو حجم معين في حالة معرفة الوسيط المستخدم في النقل . ومن هذا الجدول نستنتج أنه عندما يكون تردد النطاق كبيراً ، يمكننا إرسال ملفات ضخمة خلال فترة زمنية قصيرة

هل تعرف كيف تحسب الزمن اللازم لإرسال ملف حجمه 10G.B. عبر خط سريع من نوع STS – 48 (OC – 48) .

استخدم المعادلة التالية لحساب الزمن الذي يستغرقه نقل ملف معين .

T = S / BW

حيث

T : الزمن المستغرق لنقل الملف (Time)

S : حجم الملف (Size)

BW : تردد النطاق (Bandwidth) أو سرعة نقل الوسيط المستخدم

ومعناها اقسم حجم الملف علي تردد النطاق (Bandwidth)

إذن الزمن اللازم لنقل الملف هو

10 G.B. / 2488.32

$= 10 * 10^9 * 8 / 2488.32 X10^6 /S$

= 32.15 Seconds

العوامل التي تؤثر في سرعة نقل البيانات

الزمن المحسوب نظرياً لنقل الملف في المثال السابق يقل عملياً تبعاً لمجموعة من

العوامل التي تشترك وتؤثر في سرعة النقل . من هذه العوامل

- مواصفات وحدة الخدمة (Server) حيث تؤثر سرعة المعالج وحجم الـــذاكرة ونوعية القرص علي السرعة .
- مواصفات محطة العمل (WorkStation) التي ترسل منها البيانات .
- عدد مستخدمي الشبكة حيث يقل الأداء كلما زاد عدد مـــستخدمي الـــشبكة لزحمة "المواصلات"
- نوعية البيانات المرسلة / المستقبلة ، فعلي سبيل المثال تستغرق ملفات الـــصوت والفيديو وقتاً أطول من الملفات النصية .
- وأخيراً الطريقة المختارة لتوصيل الشبكة .

ملخص الفصل

شرحنا في هذا الفصل نظرة واسعة عن أساسيات الكمبيوتر تهم بصفة أساسية العـــاملين فى مجال الشبكات. بدأنا بشرح نظم الأعداد المشهورة والتي تهمك وهي النظـــام العـــشري والنظام الثنائي والنظام السداسي عشر. ثم شرحنا كيفية التحويل من نظام إلى آخر. شرحنا بعد ذلك كيفية حساب سرعة نقل البيانات. وأخيراً تحدثنا عن أهم نظم تشغيل الشبكات.

تدريبات

١. حول الأرقام التالية من النظام الثنائي إلى النظام العشري
110111

٢. حول الأرقام التالية من النظام العشري إلى النظام الثنائي
49

٣. حول الأرقام التالية من النظام العشري إلى النظام السداسي عشر
31644

٤. حول الأرقام التالية من النظام السداسي عشر إلى النظام العشري
B9C

٥. حول الأرقام التالية من النظام السداسي عشر إلى النظام الثنائي
5AF

٦. حول الأرقام التالية من النظام الثنائي إلى النظام السداسي عشر

1111 0101 0011 1100

٧. رتب وحدات القياس التالية من الأصغر إلى الأكبر:

كيلو بايت ــ ميجا بايت ــ بايت ــ جيجا بايت

٨. ما هو أقل وقت يستغرقه إرسال ملف حجمه **100 MB** من وحدة خدمة إلى عميـــل عبر خط الإنترنت باستخدام جهاز مودم سرعته ٣٣ كيلو بت / ثانية (استخدم المعادلة التالية **T = S/BW**)

حيث تشير **T** إلى الزمن المستغرق لنقل الملف و **S** إلى حجم الملـــف و **BW** إلى تـــردد النطاق

٩. ما هي العوامل التي تؤثر في سرعة نقل البيانات

أ. مواصفات وحدة الخدمة وعدد الأجهزة

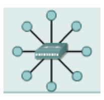
ب. عدد المستخدمين

ج. نوعية البيانات المرسلة / المستقبلة

د. مواصفات وحدة العمل

هـــ. كل ما سبق

و . لا شئ مما سبق





الشبكة المادية هي كل المعدات التي يمكنك أن تلمسها بيـــدك . يعـــد الجانب المادي من شبكة الاتصال هو المكونات المختلفة الـــتي تمكّـــن اتصال مادي فعلي بين أجهزة الكمبيوتر .

في هذا الفصل والفصل الذي يليه سنشرح بالتفصيل أجهزة ووســـائط الاتصال المادية لتوصيل شبكات الكمبيوتر ، وستتعرف علي الأشكال المختلفة للشبكات .

بانتهاء من هذا الفصل ستتعرف علي :

- *أنوا ع توصيل الشبكات وأنوا ع الشبكات*
- *الأشكال المختلفة للشبكات*
- *تصنيف الشبكات الحديثة*

أنواع توصيل الشبكات Physical Topology

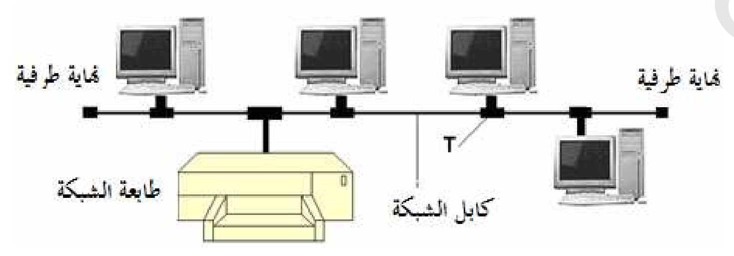
توجد ثلاثة تخطيطات من منظور توصيل الشبكات باستخدام الأسلاك النحاسية وهي تخطيط أداه النقل (**Bus Topology**) . والتخطيط ألنجمي **Star Topology** والتخطيط الحلقي **Ring Topology**. وفيما يلي توضيح لكل من هذه التخطيطات .

أولاً : تخطيط أداه الناقل Bus Topology

تعتبر شبكة تخطيط أداه الناقل من أقدم تخطيطات الشبكات. وهي بسيطة وسهلة في ربط الشبكات. وهي عبارة عن كابل طويل به أجهزة اتصال بطوله تتصل بها أجهزة الكمبيوتر (انظر شكل ٤-١) وبمجرد أن يتم توصيل أجهزة الكمبيوتر بالأسلاك وتثبيت برامج الشبكة علي أجهزة الكمبيوتر ستتمكن أجهزة الكمبيوتر من رؤية بعضها البعض. يتم وضع وصلة علي كل طرف من أطراف السلك كما يظهر من شكل ٤-١ تسمي هذه الوصلة "نهاية طرفية " . تقوم النهاية الطرفية بامتصاص أي إشارة تصل إليها وبالتالي يصبح السلك خالياً من أي إشارة ويصبح مستعداً لاستقبال أي معلومات مما يمكن أي جهاز آخر من إرسال بياناته علي الشبكة .

تستخدم أنظمة **Ethernet** القديمة تخطيط أداة النقل مع الكابلات المحورية (**Coaxial**) ومن عيوب هذه الشبكة أنه إذا تم قطع أي من الارتباطات بين أجهزة الكمبيوتر، سوف تنهار الشبكة.

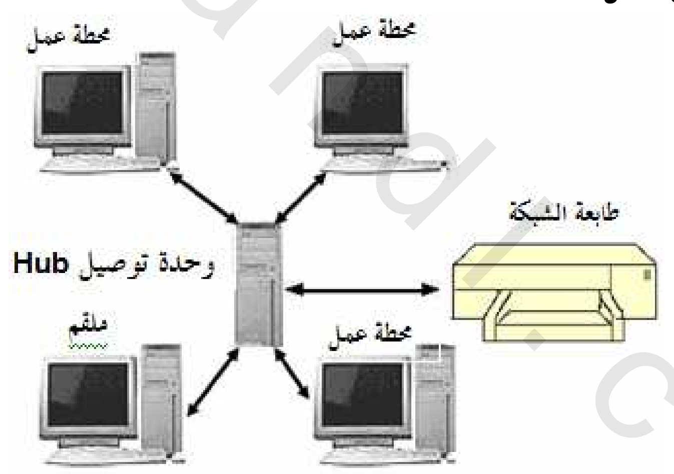
تعد تخطيطات أداه الناقل من أقدم تخطيطات الشبكات وأكثرها فشلا. وكذلك من الصعب توسيعها. ولذلك لم تعد هذه التكنولوجيا مستخدمة بعد أن تحول المستخدمون إلى تكنولوجيا التخطيطات النجمية والحلقية.



شكل ٤-١ تخطيط شبكة أداة النقل **Bus Topology**

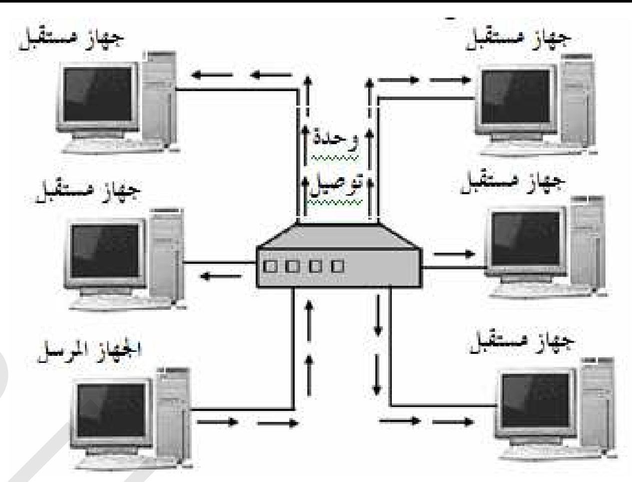
ثانياً : التخطيطات النجمية Star Topology

يعتبر هذا التخطيط أفضل من التخطيط السابق لأنه أكثر قوة وأقل تعرضا للفشل . لايعتمد التخطيط النجمى علي نظام السلك الذي يربط أجهزة الكمبيوتر كما في تخطيطــات أداه النقل السابقة. وإنما يستخدم علبة كهربية يطلق عليها hub أو Switch لتوصيل أجهزة الكمبيوتر ببعضها البعض (انظر الشكل ٤-٢) ولهذا فهو يتميز عن الــسابق. حيــث في تخطيط أداه النقل يتسبب قطع اتصال جهاز كمبيوتر واحد في انهيار الشبكة بأكملها، أما في التخطيط النجمي فإن نظام توصيل الأجهزة بوحدة التوصيل يعزل كل سلك من أســلاك الشبكة عن الآخر، وبالتالي إذا توقف جهاز أو انقطع السلك الذي يربطه بوحدة التوصيل فلن يتأثر إلا الجهاز الذي توقف أو انقطع سلكه . أما باقي الأجهزة فستبقي تعمل وتتبادل البيانات فيما بينها . أما إذا توقف جهاز التوصيل (Hub) أو فشل فإن الشبكة كلــها ستتوقف عن العمل .



الشكل ٤-٢ التخطيط النجمي للشبكات Star Topology

في التخطيط النجمي يمكنك توصيل أجهزة الكمبيوتر أثناء التشغيل دون التسبب في فشل الشبكة. حيث يتصل كل جهاز بوحدة التوصيل (الــ Hub أو الــ Switch) بواســطة كابل منفصل. تنتقل الإشارات من الجهاز المرسل إلي وحدة التوصيل ومنه إلي باقي الأجهزة علي الشبكة كما يتضح من شكل ٤-٣ .



شكل ٤-٣ انتقال الإشارة من وحدة التوصيل إلي باقي الأجهزة

تستخدم العديد من أبنية الشبكات التخطيط النجمى. أشهر هذه الأبنية **Ethernet** سواء الإصدار القديم منها أو الإصدار الجديد مثل **100Base–T** وتخطيط **Gigabit Ethernet**

ثالثاً : التخطيطات الحلقية Ring Topology

في التخطيط الحلقي (**Ring Topology**) يتم ربط الأجهزة في الشبكة بحلقة أو دائرة من السلك بدون نهايات كما يتضح من الشكل ٤-٤. تنقل الإشارات علي مدار الحلقة في اتجاه واحد وتمر من خلال كل جهاز علي الشبكة . ويقوم كل جهاز علي الشبكة بإنعاش الإشارة التي تمر من خلاله وتقويتها ثم يعيد إرسالها علي الشبكة إلي الجهاز الذي يليه .

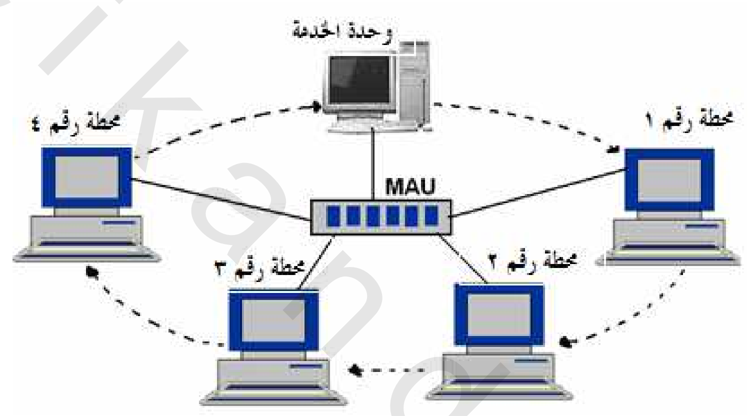
أشهر أبنية الشبكات التى تستخدم التخطيط الحلقى هي شبكات **Token Ring** وشبكات **FDDI**. ويتم ترتيب التخطيطات الحلقية فى نفس النجمة المادية التى تجدها فى شبكات التخطيط النجمى **Ethernet**.

علي الرغم من أننا نميز بين تخطيط**Star** (النجوم) و**Ring** (الحلقات) فأنهما من الناحية المادية يبدوان متشابهين. للشبكات الحلقية أيضا نقطة اتصال مركزية تتصل بها أجهزة الكمبيوتر. شكل (٤-٤)

في شبكة **Token Ring** يتم توصيل كل الأجهزة بواسطة أسلاك إلي نقطة واحدة هي **Token Ring MAU**. حيث **MAU** اختصار لعبارة **Multistation Access Unit**

ويمكن ترجمتها (وحدة وصول متعددة المحطات). تشبه **MAU** وحدة التوصيل **(hub)** أو السويتش في أنها توفر منافذ لتوصيل أجهزة الكمبيوتر ماديا علي الشبكة . كما يتضح من (شكل٤-٤). تنقل **MAU** البيانات من جهاز كمبيوتر إلي أخر في مسار يكـــرر حلقـــة. (ولهذا يطلق على **Token** اسم **Ring** ومعناها حلقة).

أما بناء الشبكة الآخر الذى يستخدم التخطيط الحلقى فهو شـــبكات **FDDI** أو **Fiber Distribution Data Interface** ومعناها "واجهة البيانات الموزعة لشبكة الألياف". إلا أن بناء شبكة **FDDI** يعمل على كابلات ألياف بصرية بدلا من الكابلات النحاسية.



شكل ٤-٤ مخطط شبكة التخطيط الحلقي **Token Ring**

تتميز بنية **FDDI** بعدة مميزات: السرعة إذا ما قورنت ببنية **Ethernet** والحد من الفشل الذى يحدث فى اتصالات الشبكة ويمكن الاعتماد عليها . ولكنها تعد أيضا باهظة التكاليف مقارنة بمقياس **Ethernet-F** التي تستخدم الألياف البصرية .ولعل هذا هو السبب الذي أدي إلي انتشار واستخدام **Ethernet** بصورة أكبر .لتقنية **FDDI** حلقتين كاملتين يطلق عليهما الحلقة الأولية (**Primary**) والحلقة الثانوية (**Secondary**) وهمـــا تعمـــلان في اتجاهين متقابلين . يوفر زوجا الحلقات قدراً أساسياً من الوقوع في الأخطاء . فإذا كانـــت إحدى الحلقات مقطوعة ، فستتولى الحلقة الأخرى المهمة . وإذا كان أحد مقاطع الحلقتين مقطوعاً أو إذا لم يعمل أحد الأجهزة أو تمت إزالته ، يمكن ربط الحلقتين لإعادة تأســـيس تكامل الحلقة .

أنواع الشبكات

يمكن تقسيم الشبكات التي تستخدمها المؤسسات إلي شبكات محلية (**LAN**) وشـــبكات واسعة (**WAN**) وهذا بخلاف الشبكة العالمية المعروفة باسم "شبكة الانترنت" حيث يمكن الاتصال بالانترنت بدون أي من الشبكتين كما يمكن توصيل شـــبكة المؤســـسة بـــشبكة الانترنت. وفيما يلي نوضح باختصار أهم أنواع الشبكات.

الشبكة المحلية (LAN)

باختصار شديد عندما يتم توصيل أكثر من جهاز كمبيوتر مع بعضهم من خـــلال شـــبكة توجد كلها في موقع واحد تسمي هذه الشبكة شبكة اتصالات محلية أو **Local Area Network** وتختصر هكذا **LAN**.

يمكنك اعتبار الشبكات التي اشرنا إليها في هذا الفصل (الشبكة الخطيـــة أو الحلقيـــة أو النجمية) شبكات محلية

وتتميز شبكة الاتصالات المحلية (**LAN**) بما يلي :

- توجد كلها في مكان واحد أو قريب ولهذا نقول عنها "محلية" .
- تتميز بمعدل عالي لنقل البيانات يصل إلي ١٠٠٠ميجابت في الثانية.
- تنتقل البيانات عبر أسلاك الشبكة.

يمكن أن تشمل شبكة **LAN** علي المئات أو الآلاف من المستخدمين رغم وجودها في موقع جغرافي واحد.

شبكة الاتصال الواسعة (WAN)

كلمة **WAN** اختصار لعبارة **Wide Area Network** وتعني شبكة الاتصال الواســـعة. ومن هذا الاسم تعرف أنها أوسع من الشبكات المحلية.

عندما تزيد فروع الشبكة وتتباعد في أكثر من مدينة (لم تعد في مكان واحد) فلابـــد مـــن إنشاء عدة شبكات محلية وتوصيل هذه الشبكات مع بعضها.

عندما تتطلب المؤسسة توصيل أكثر من شبكة **LAN** مع بعضها نظرا لبعد المـــسافة بـــين فروعها أو مراكزها. هنا لا مفر من إنشاء شبكة اتصال واسعة (**WAN**).

إذن شبكات **WAN** عبارة عن شبكات **LANs** موزعة جغرافيا يتم ربطها معا باستخدام اتصالات داخلية عالية السرعة وموجهات.

علي عكس شبكة **LAN** ، تتطلب شبكة **WAN** موجهات (**Routers**) تقوم الموجهات بوظيفة التحكم في تدفق الاتصالات .

إذن الموجه جهاز يدير تدفقات البيانات بين الشبكات. تقوم الموجهات(**Reuters**) بنقل البيانات من نقطة إلي أخري وتعرف أفضل مسارات التوجيه لنقل البيانات، ولكي تفهم عمل الموجه أكثر. افرض انك تسير في طريق ونتيجة للزحام الشديد تم تغيير مسار الطريق. ستجد علامات مرور بطول الطريق توجهك لكي تسلك الطريق المناسب والبديل . هذه العلامات تعمل عمل الموجه الذي يعرف أفضل مسارات التوجيه لنقل البيانات كما أنه يتعرف علي مسارات توجيه جديدة.

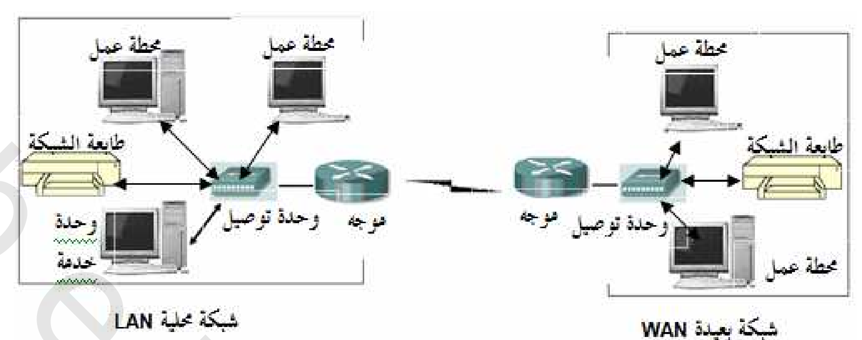
غالبا ما تتحكم سرعة خط الهاتف في سرعة نقل البيانات عبر شبكة **WAN** فبينما تعمل الشبكة المحلية (**LAN**) بسرعة ١٠٠ميجا بت في الثانية فإن سرعة خط الهاتف تعمل بسرعة ٥٦ كيلو بت في الثانية وفي أحسن الأحوال في حالة الخطوط التي يتم تأجيرها بآلاف الجنيهات شهريا من شركة الاتصالات (خط **T1**) تصل سرعة خط الهاتف إلي ١,٥ميجا بت في الثانية. عندما تقارن سرعة شبكة محلية تعمل بسرعة ١٠٠ميجابت في الثانية بسرعة خطوط الهاتف الرقمية يتضح لك بطء خطوط الهاتف الرقمية .

يطلق علي سرعة نقل البيانات مصطلح (تردد النطاق). ولذلك فإن تردد النطاق الذي ينقل ١,٥ميجا بت في الثانية أعلي من تردد النطاق الذي ينقل ٥٦كيلو بت في الثانية (لاحظ الفرق في السرعات) ولذلك يشتكي المستخدمون من بطء نقل البيانات (غالبا ما يقولون الجهاز بطيء) عندما تزيد كمية البيانات المطلوب نقلها عن سعة خط الهاتف.

أما إذا كانت كمية البيانات المطلوب نقلها أقل من سعة الخط أو تساويها فلن تحصل مشكلة. نظرا لأن تدفق البيانات في شبكات **WAN** يتم داخل شبكات **LAN** التي تتكون منها شبكة **WAN** فقد برزت الحاجة إلي الموجهات لكي تتحكم في تدفق الاتصالات.

يشتمل شكل (٤–٥) علي رسم تخطيطي لشبكة **WAN** ومنه تلاحظ أن شبكة **WAN**

عبارة عن مجموعة من شبكات LAN متصلة ببعضها عن طريق موجه .

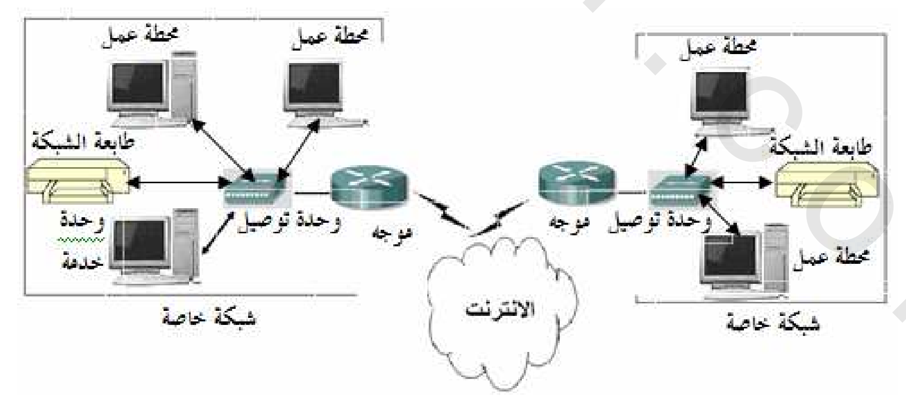


شكل ٤-٥ ربط الشبكات المحلية LAN بالشبكات الموسعة WAN

شبكة الانترنت

أصبحت الانترنت هوس عالمي، حيث لم يعد شخص في العالم لم يسمع عن الانترنت وزاد مستخدموها في العالم زيادة هائلة في السنوات الأخيرة أما مستخدموها في العالم الثالث، فما زالوا يبحثون عن لقمة العيش قبل البحث عن خط الهاتف الذي يمكنهم من الاتصال بالانترنت.

تستخدم الشركات شبكات خاصة بها سواء كانت من نوع LAN أو حتي من نوع WAN ويتم توصيل هذه الشبكات بشبكة الانترنت عن طريق توصيل موجه بالشبكة والاتصال بشبكة الانترنت من خلال مزودي خدمة الانترنت. انظر شكل ٤-٦



شكل ٤-٦ توصيل الشبكات بشبكة الانترنت عن طريق موجه

كيفية الاتصال بالانترنت

يمكن الاتصال بالانترنت بأكثر من طريقة

- **بعض الناس الذين يتصلون بالانترنت من منازلهم يستخدمون مــودم Modem أمــا الشركات الصغيرة فأنهم غالبا ما يستخدمون كابل أو DSL للاتــصال بالانترنــت. وبالطبع فإن الكابل والـــــ DSL أكثر مناسبة للشركات التجارية الصغيرة لأنه يوفر تردد نطاق أكثر مما يوفره المودم الموجود بجهاز الكمبيوتر الذي يستخدمه الأفــراد في منازلهم. ففي حين تصل سرعة الاتصال عن طريق المودم إلي ٥٦ كيلو بت في الثانيــة، تصل سرعة الكابل والــــ DSL إلي ٥٠٠ كيلو بت في الثانية أو أكثر.**
- **أما الشركات ألكبري والمؤسسات فإنها تستطيع الحصول علي سرعة عالية عن طريــق تأجير خطوط اتصالات رئيسية. هذه الخطوط يمكن إن توفر تردد نطاق يــصل إلي ١,٥ ميجا بت في الثانية كما أشرنا سابقا.**

تصنيف الشبكات الحديثة

تنقسم الشبكات الحديثة إلي نوعين :

- ***الشبكات النظيرة Peer to Peer Networks***
- ***شبكات الوحدة التابعة/وحدة الخدمة Client / server Network***

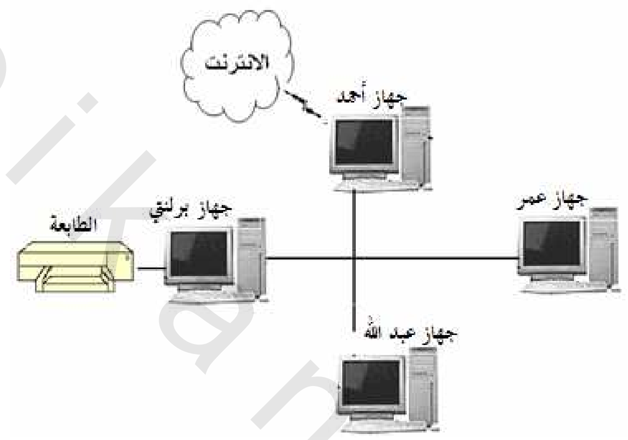
وفيما يلي نوضح ما هي الشبكة النظيرة وما هي شبكة الوحدة التابعة / وحــدة الخدمــة (شبكة العميل/الخادم) .

الشبكة النظيرة Peer to Peer Networks :

من اسم هذه الشبكة أن كل جهاز فيها يناظر الجهاز الآخر. وهي عبارة عن شبكة محليــة مكونة من مجموعة أجهزة لها نفس الحقوق والواجبات (متناظرة). ولذلك فهي لا تحتاج إلي وحدة خدمة (server) حيث أن كل جهاز في الشبكة قادر علي استقبال بيانات وفي نفس الوقت قادر علي تزويد غيره من الأجهزة بالمعلومات

فعلي سبيل المثال قد تستخدم واحد من الأجهزة عليها قرص صلب كبير لتخزين بيانــات

جميع المستخدمين كما قد تستخدم طابعة متصلة بأحد الأجهزة مع باقي المستخدمين. في المثال الموضح بشكل ٤-٧ يتصل جهاز أحمد بالانترنت، ويتوفر لجهاز أسامة طابعة يمكن لجميع الإفراد استخدامها، كما يوجد قرص صلب علي جهاز عمر تخزن عليه ملفات وبيانات جميع المستخدمين. في حين يستطيع جهاز عبد الله الاستفادة من الخدمات التي يقدمها أي من الأجهزة الثلاثة.



شكل ٤-٧ شبكة نظيرة تتصل جميع الأجهزة ببعضها

ومن مميزات الشبكة النظيرة :

- التكلفة المادية المحدودة مقارنة بشبكات(الوحدة التابعة/ وحدة الخدمة أو العميل/الخادم).
- سهولة تجهيز الشبكة وإعدادها للعمل.
- لا تحتاج لبرامج أخرى غير نظام التشغيل المستخدم.
- تلاءم الشبكات الصغيرة جداً (من ٣ -٤ أجهزة).

أما عن عيوبها فهي لا تستوعب إلا عدد محدود من الأجهزة ويعد الأمان في الشبكة النظيرة غير موجود تقريبا. كما أنه لا يمكن الاعتماد عليها حيث يسهل تشويشها.

***شبكات الوحدة التابعة/ وحدة الخدمة* Client/server *Network*.**

تسمي شبكات الوحدة التابعة / وحدة الخدمة أحياناً "شبكة العميل / الخادم" ، تعتمد هذه الشبكات علي جهاز يسمي **Server** أو وحدة الخدمة أو الخادم أو الملقم تتصل به

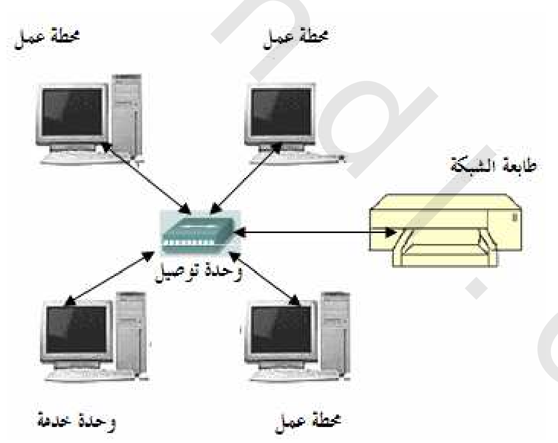
الأجهزة التي تعمل كمحطات أو كوحدة تابعة داخل الشبكة. عادة تكون وحدة الخدمة أو جهاز الخادم جهاز كبير وذو ذاكرة كبيرة ومعالج قوي. وقد يحتوي علي معالجين عندما يكون عدد الأجهزة كبير في الشبكة، يمكن تزويد الشبكة بأكثر من وحدة خدمة (Server)

يشتمل شكل ٤–٨ علي شبكة تستخدم وحدة خدمة .

ومن فوائد هذا النوع من الشبكات

- يمكنها تدعيم آلاف المستخدمين
- توفير حماية وسرية أكثر للبيانات
- إدارة مركزية لموارد الشبكة

أما من عيوب هذه الشبكة فأهمها الإمكانيات المادية، حيث تتكلف وحدة الخدمة مبالغ هائلة رغم أنه لا يستخدم من أي فرد مثل محطة العمل، وإذا تعطلت وحدة الخدمة سوف تتعطل الشبكة كلها .



شكل ٤–٨ شبكة "وحدة خدمة / وحدة تابعة " تستخدم وحدة خدمة تتصل بها الوحدات التابعة

ملخص الفصل

شرحنا في هذا الفصل أنواع توصيل الشبكات وقلنا أن هناك ثلاثة تخطيطات لتوصيل الشبكات هي تخطيط أداة النقل **Bus Topology** والتخطيط النجمي **Star Topology** والتخطيط الحلقي **Ring Topology** وأوضحنا الفرق بين كل نوع من هذه الأنواع الثلاثة . شرحنا بعد ذلك أنواع الشبكات وقسمناها إلى شبكات محلية (**LAN**) وشبكات واسعة (**WAN**) وشبكة الإنترنت . شرحنا أيضا تصنيف الشبكات إلى شبكات نظيرة وشبكات الوحدة التابعة / وحدة الخدمة.

تدريبات

١. ما هي التخطيطات المادية المستخدمة على شبكات الكمبيوتر (اختر ثلاثة):

أ. تخطيط البناء الهرمي

ب. تخطيط أداة النقل

ج. التخطيط الأفقي

د. التخطيط النجمي

هـ-التخطيط الحلقي

و- التخطيط الرأسي

٢. عند مقارنة تخطيطات الشبكات يمكن أن نقول:

أ. تخطيط أداة النقل	١. يوفر هذا التخطيط حلقة منطقية تنقل البيانات في مسار دائري من جهاز لآخر. أشهر بنية شبكات تستخدم هذا التخطيط هي شبكات **TokenRing** و **FDDI**
ب. التخطيط النجمي	٢. أشهر بنية شبكات تستخدم هذا التخطيط هي شبكة **Ethernet**. إذا انقطع أي ارتباط لا يتأثر إلا الجهاز الذي توقف أو انقطع سلكه
ج. التخطيط الحلقي	٣. يعتمد على نظام السلك الذي يربط بين الأجهزة

ولذلك إذا انقطع أي ارتباط بين الأجهزة، تنـــهار الشبكة وتستخدمه شبكات ETHERNET القديمة.

٣. ما هو الفرق الجوهري بين شبكات LAN وشبكات WAN

٤. يمكن تقسيم الشبكات من حيث طريقة توصيلها إلى نوعين هما ...... و ....

٥. صح أم خطأ:

أ. توفر الشبكات النظيرة أكبر حد من الأمان ويمكن الاعتماد عليها

ب. شبكة الوحدة التابعة / وحدة الخدمة تلائم الأجهزة والشبكات الصغيرة جـــداً (من ٣ ــ ٤ أجهزة)

ج. لا تحتاج الشبكة النظيرة إلى برامج أخرى غير نظام التشغيل المستخدم

د. من عيوب شبكات الوحدة التابعة / وحدة الخدمة إنها لا تـــوفر إدارة مركزيـــة لإدارة الشبكة

هـــ. يمكن أن تدعم شبكات الوحدة التابعة / وحدة الخدمة آلاف المستخدمين



الباب الثاني

المفاهيم الأساسية لربط الشبكات

الفصل الخامس : تقنيات الشبكات المحلية

الفصل السادس : نموذج **OSI**

الفصل السابع : النموذج المرجعي العملي للاتصال بالانترنت **TCP/IP**



*ناقش في هذا الفصل تقنيات الشبكة المحلية. سنركز على تقنية **Ethernet** باعتباره السائد الآن والأسهل والأرخص . نشرح كذلك التقنيات الأخرى مثل **Token Ring** و**FDDI** وتقنية **ATM** ونختم الفصل بالحديث عن تقنيات ربط الشبكات المنزلية.*

بانتهاء هذا الفصل ستتعرف على:

- *مقياس **Ethernet***
- *تقنية **CSMA/CD***
- *أجهزة **Ethernet***
- *وسيلة الوصول إلى وسائط **Ethernet***
- *مقياس **Token Ring**و**FDDI***
- *مقياس **ATM***
- *ربط الشبكات المنزلية*
- *بروتوكول **PPP***

شرحنا أنواع توصيل الشبكات مثل تخطيط النجمة **Star Topology** والتخطيط الحلقي **Token Ring** وتخطيط أداة النقل ، وكلها تتعلق بتوصيل الأسلاك . وفي هذا الفصل سنشرح المواصفات القياسية والتقنية للشبكات المحلية.

ولكن ما هي تقنيات الشبكة المحلية. هذه التقنيات لا تعدو أن تكون قواعد يتم وضعها لنقل البيانات حتي لا تصير الشبكة فوضوية. بعبارة أخرى هي القواعد الأساسية التي تستخدمها بعض مكونات الشبكة مثل بطاقة الشبكة والأسلاك لتنفيذ مهمتها. تتعامل تقنيات الشبكة المحلية مع طبقة ربط البيانات (**Data Link**) بأكملها وبعض من طبقتى المادية (**Physical**) والشبكة (**Network**) . (راجع طبقات نموذج **OSI** فى الفصل الرابع).

تقنية Ethernet

تعتمد تقنية شبكات **Ethernet** علي مقياس **802.3** لتقنية **Ethernet** (**Ethernet 802.3**) وهو المقياس الذي تم تخصيصه من قبل **IEEE** وهذه الحروف اختصار لعبارة **Institute of Electronic and Electrical Engineers** ومعناها بالعربية "جمعية مهندسي الكهرباء والالكترونيات". وتبنته منظمة **ISO** العالمية مما جعله مقياسا عالميا. وكان الهدف من **Ethernet** إيجاد طريقة لإدارة المشكلة التى تحدث عندما يحاول أكثر من جهاز كمبيوتر نقل البيانات على سلك واحد فى وقت واحد.

أصبح **Ethernet** هو تقنية الشبكات المحلية السائدة على نطاق واسع نظرا لأنه رخيص نسبياً ويسهل توسيعه إلى شبكات اتصال كبيرة، وتستخدمه العديد من نظم الكمبيوتر. ولعل هذا هو السبب فى إزاحة التقنيات القديمة واختفائها (مثل تقنية **Token Ring**). ونتيجة لذلك فإن الكثير من البرامج ومنها على سبيل المثال **Windows Server 2003** أصبحت تدعم هذه التقنية ومعداتها.

نتناول فيما يلى تقنية **Ethernet** من النواحي التالية :

أولا: التقنية المستخدمة للتحكم فى تدفق البيانات والتى تسمى **CSMA/CD** وهى عبارة عن وسيلة للوصول إلى وسائط ايثرنت.

ثانيا: أجهزة ايثرنت

ثالثاً : أطر ايثرنت Ethernet Frames

أولا : مقياس CSMA/CD:

تحتاج ايثرنت إلى وسيلة تصف كيفية مشاركة أكثر من جهاز كمبيوتر لقناة ايثرنت واحدة لأن الهدف من ايثرنت هو جعل أجهزة كمبيوتر متعددة تعمل بصورة مستقلة عن بعضها البعض عبر قناة اتصال واحدة دون تدخل . تستخدم Ethernet فى ذلك وسيلة وصول للوسائط تسمى CSMA/CD. كلمة CSMA/CD اختصار للعبارة
Carrier Sense Multiple Access/Collision Detection
ومعناها بالعربية "اكتشاف الوصول المتعدد/التعارض لتحسس الحامل" ونوضح فيما يلى هذا المقياس

طريقة عمل مقياس CSMA/CD

١. يشير" Carrier Sense "(استشعار حالة خط الاتصال) إلى أنه متى رغب جهاز كمبيوتر في إرسال بيانات عبر كابل الشبكة فإنه يستشعر حاله الكابل أولا لمعرفة ما إذا كان هناك جهاز آخر يحاول الإرسال أيضا أم لا .
٢. إذا اكتشف الجهاز أن خط الاتصال خالي، فإنه يدرك أنه يمكن استخدامه في إرسال البيانات التي يرغب فيها. ويقوم بوضع المعلومات الخاصة به على شبكة الاتصال باستخدام عنوان الوجهة مما يجعلها متاحة لكل أجهزة الكمبيوتر الأخرى على الشبكة.
٣. يفحص كل كمبيوتر موجود على شبكة الاتصال ما إذا كان العنوان يخصه أم لا، فإذا كان يخصه، يسحب المعلومات خارج الشبكة.
٤. عندما يصبح خط الاتصال خاليا مرة أخرى، تصبح لكل أجهزة الكمبيوتر الأخرى فرصه متساوية لأن تكون التالية فى نقل المعلومات.
٥. عندما يحاول جهازي كمبيوتر نقل حزم بيانات على نفس أسلاك الشبكة في نفس الوقت، تحدث حالة يطلق عليها " تعارض". هذا التعارض يتسبب في توقف النقل لأن كلا من جهازي الكمبيوتر يحس بهذا التعارض .وتتم إعادة شبكة الاتصال إلي حالتها غير النشطة .

وعادة تشترك كل أجهزة الكمبيوتر في مقطع شبكة واحد يطلق عليه. "نطاق التعارض" ويعتبر المقطع الذي تشترك فيه أجهزة الكمبيوتر داخل الشبكة نطاق تعارض. وذلك لأن أجهزة الكمبيوتر الموجودة على نفس النطاق تحاول إرسال بياناتها في نفس الوقت. و هو ما ينتج عنه التعارض.

وعادة لا يمكن لجهاز الكمبيوتر نقل البيانات عندما يكون هناك جهاز كمبيوتر آخر يجرى عملية نقل في نفس الوقت ولكن الذي يحصل أنه ينتظر لفترة عشوائية لحين يحدث هدوء على الأسلاك (هذا الهدوء يقاس بالنانو ثانية). فإذا حصل هدوء لأسلاك الشبكة يتم إرسال حزم البيانات عبر أسلاك الشبكة. يشترط ألا ترسل أية أجهزة أخرى أى بيانات. إما إذا حاول جهاز آخر نقل بيانات في نفس الوقت الذي ينقل فيه الجهاز الأول البيانات فسوف يتوقف كلاهما عن نقل البيانات ويتم الانتظار لفترة من الوقت حتى يحصل هدوء ثم ينقلان البيانات. كلما زاد نطاق التعارض (عدد أجهزة الكمبيوتر فى أى مقطع) زاد احتمال حدوث تعارضات ولهذا السبب يحاول مصمموا **Ethernet** الاحتفاظ بأقل عدد من الأجهزة الموجودة فى أى مقطع.

وبالرغم من كل ماقلناه، فإن الأمر لايخلو من وجود بعض المشكلات لمقياس **CSMA/CD** مثلاً إذا كانت بطاقة الشبكة بها عيب، فإنها تفشل فى الاستجابة لـ **CSMA/CD** وأيضا إذا كان عدد أجهزة الكمبيوتر فى مقطع واحد كبيرا، فستحاول العديد من الأجهزة النقل فى نفس الوقت، ويمكن أن يسبب هذا مايسمى **Broadcast Storm** "اندفاعات بث" وللتغلب على مثل هذه المشكلة نضطر لتجزئة الشبكة إلى مقاطع باستخدام تقنيات أجهزة التبديل **(Switches)** راجع أجهزة التبديل **(Switches)** فى الفصل الثامن .

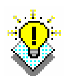
ثانيا: أجهزة شبكة Ethernet

تستخدم تقنية **Ethernet** سبعة مقاييس للأجهزة.(٧ أنواع من الشبكات داخل عائلة **Ethernet**).يستخدم كل مقياس أجهزة نوع محدد من الكابلات وتخطيطات الكابلات ويوفر سرعة على شبكة الاتصال تقدر بالميجابت/ثانية. ويحدد حداً أقصى لطول المقطع

ولعدد الأجهزة على المقطع الواحد. نستعرض فيما يلى عائلة Ethernet لتكون على دراية بما يناسبك منها.

- **10Base2** و **10Base5** : تعد كلا منهما تكنولوجيا قديمة. ولم تعد تستخدم فى عمليات التركيب الحديثة. فى شبكات 10Base2 يصل أقصى طول للمقطع ١٨٥مترا، بما يصل إلى ٣٠ كمبيوتر فى المقطع الواحد وبما يصل إلى ثلاثة مقاطع. ويستخدم فيها الكابل المحورى الرفيع (Thin Coaxial).

أما فى شبكات 10Base5 فيصل أقصى طول للمقطع ٥٠٠ مترا ويستخدم فيها كابلات من النوع المحورىThick Coaxial تعمل كلتا الشبكتين نظريا على نقل البيانات بمعدل ١٠مليون بت فى الثانية (10Mbps).



فى أسماء IEEE الخاصة بمقاييس أجهزة Ethernet مثل 10Base5 تشير 10إلى السرعة بالميجابت، بينما تشير Base إلى Baseboard (التردد الأساسي)، ونوع النقل وتشير 5 إلى الحد الأقصى لطول المقطع بالمائة متر. فى المقاييس الحديثة مثل 10BaseT ترمز T أو F لنوع الكابلات. حيث يشير الحرفTإلى كابل UTP وهو الكابل المجدول غير المحمي . بينما يشير الحرف F إلي كابل الألياف البصرية Optical Fiber

- **10BaseT** : تعد تكنولوجيا 10BaseT أيضا تكنولوجيا قديمة ويبلغ أقصى طول للكابل بين أى محطة ووحدة التوصيل (Hub) ١٠٠متراً . تستخدم الأسلاك المزدوجة المجدولة غير المحمية(Unshielded Twisted Pair (UTP تبلغ سرعتها ١٠ميجابت فى الثانية. لاحظ هنا أن T تشير إلي نوع الكابل UTP بينما تشير 10 إلي السرعة بالميجابايت
- **10BaseF** : تستخدم كابل ألياف بصرية (تشير F إلي Optical Fiber) يعمل بسرعة ١٠ميجابت فى الثانية، لتوصيل شبكتى اتصال تبعدان عن بعضهما بمسافة ٤٠٠ متر. غالبا ما تستخدم لتوصيل أكثر من مكان داخل منطقة واحدة.
- **100BaseT** : يطلق على هذا النوع من الشبكات Fast Ethernet أو ايثرنت السريعة. تبلغ سرعة نقل البيانات ١٠٠ ميجابت فى الثانية أي أن سرعته تزيد عن سرعة

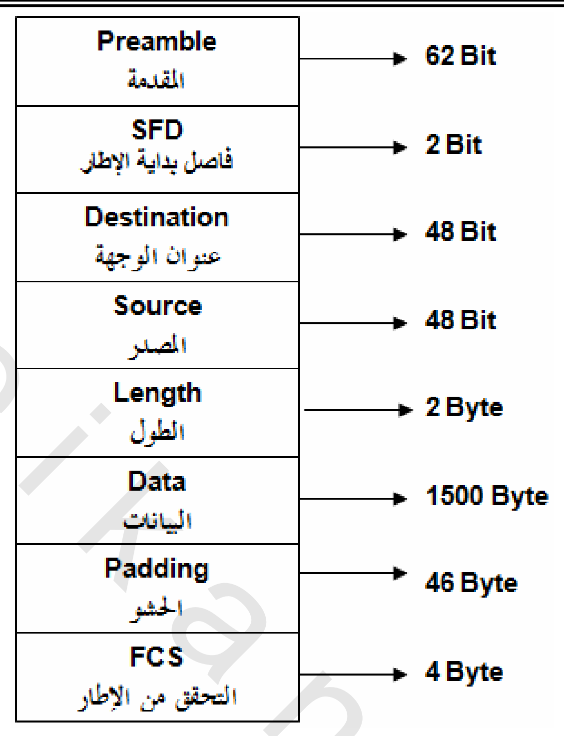
10BaseT بعشر مرات. يبلغ أقصى طول للكابل بين أى محطة ووحدة التوصيل ٢٠ متراً. تستخدم الأسلاك النحاسية المزدوجة المجدولة غير المحمية (UTP).وتتطلب مقاييس توصيل الكابلات Category 5 (الفئة ٥). لا تزيد تكلفة 100BaseT عن 10BaseT بكثير رغم سرعتة الإضافية. ولذلك أصبح هو مقياس أجهزة اثيرنت.

- **100BaseFX و 100BaseFL : تستخدم هذه الشبكات الألياف البصرية لنقل البيانات ولذلك فهى تحمل البيانات إلي مسافة أبعد مما تحملها الأسلاك النحاسية وتعمل بسرعة ١٠٠ميجابت فى الثانية . وتستخدم لتوصيل شبكتان تبعدان عن بعضهما مايصل إلى ٤٠٠ مترا.**
- **1000BaseT و1000BaseF : يطلق عليها "جيجابت اثيرنت" Gigabit Ethernet نظرا لسرعتها العالية التى تبلغ ١٠٠٠ميجابت فى الثانية أى جيجابت فى الثانية(1Gbps) أى أنها أسرع ١٠مرات من النوع 100BaseT والذى يطلق عليه Fast Ethernet "ايثرنت السريع".**

تستخدم أسلاك نحاسية من نوع Cat 5 (فئة٥) أو Cat 6 (فئة٦) أو كابل ألياف ضوئية. تستخدم مقاييس مسافات متعددة تتراوح بين ٢٥ مترا، ١٠٠ مترا للكابل UTP (الكابل المزدوج المجدول غير المحمى). تستخدم 1000Base-T بكثرة لوحدات الخدمة والشبكات الأساسية للمعلومات. أما فى المستقبل القريب فلا ندرى ماتخبئه التكنولوجيا القادمة من مفاجآت.

ثالثاً : أطر ايثرنت Ethernet Frames

عندما يستلم إيثرنت تخطيط البيانات من طبقة الشبكة يقوم بتغليف البيانات داخل إطار (Frame). يحدد هذا الإطار معلومات الرأس وعنونة مصدر البيانات ومعلومات التذييل كما يتضح من الشكل ٥-١



شكل ٥-١ إطار ايثرنت

نوضح فيما يلى حقول إطار إيثرنت واستخداماتها

- مقدمة **Preamble** : سلسلة من أرقام الآحاد والأصفار المتناوبة التى تستخدم من قبل الجهاز المستقبل لضبط تزامن المعلومات فى الإطار.
- فاصل بداية الإطار **start of Frame Delimiter (SFD)** : رموز ثنائية تستخدم للدلالة على بدء عملية الإرسال الفعلية.
- عنوان الوجهة **Destination Address** : يحتوى على عنوان طوله ٦ بايت يمثل عنوان بطاقة شبكة جهاز المستقبل. ويكتب العنوان بالنظام السداسى عشر .
- عنوان المصدر **Source Address** : أيضا طوله ٦ بايت ويحتوى على عنوان الجهاز المرسل للبيانات.
- الطول **Length** : حقل طوله ٢ بايت يدل على طول حقل البيانات المرسلة والتى تمثل البيانات الواردة من طبقة الشبكة فى الجهاز المرسل.

- **البيانات Data : البيانات التى يتم نقلها والتى يتراوح طولها بين صفر و ١٥٠٠ بايت.**
- **الحشو Padding : يكون هذا الحقل ضروريا فى حالة البيانات التى يقل طولها عن ٤٨ بايت. فمثلا إذا احتوى حقل البيانات على ٤٢ بايت فيتم تضمين ٦ بايت إضافية لحقل البيانات.**
- **التحقق من الإطار Frame check sequence (FCS) : عبارة عن رقم يبلغ طوله ٤ بايت يتم اشتقاقه من كل البتات الموجودة فى النقل باستخدام صيغة معقدة. يحسب الجهاز المرسل هذا الرقم ويضيفه فى الإطار المرسل إلى جهاز آخر، ويقوم الجهاز المستقبل بحساب الرقم ويقوم بمقارنته بالرقم الموجود فى الإطار. إذا لم يوجد تعارض فى الأرقام، فهذا معناه أن البيانات المنقولة صحيحة. ويتم استلامها، وإذا كانت مختلفة يتم تكرار النقل.**

***عنوان المصدر وعنوان الوجهة فى إطار* Ethernet.**

يقال عنه MAC Address أو "عنوان MAC" وكلمة MAC مأخوذة من العبارة Media Access Control ومعناها بالعربية "التحكم في وصول الوسائط" وهو عبارة عن رقم يبلغ طوله ٦ بايت أو ٤٨ بت لكل منهما كما يظهر من شكل ٥-٢ يمثل كل منهما عنوان MAC لأجهزة الكمبيوتر المرسلة والمستقبلة. يتم تعيين هذه الأرقام من قبل IEEE للشركات المصنعة لبطاقات الشبكة . تحتوى الـ ٢٤ بت الأولى على رقم فريد للشركة المصنعة والـ ٢٤ بت الثانية تحتوى على رقم فريد لبطاقة الشبكة.

هذا معناه أن كل بطاقة شبكة يخصص لها رقم فريد يعتبر عنوان لها وأن المستخدم النهائى لا يقلق بخصوص هذا العنوان.

رغم أنه لا يمكنك تغيير العنوان المادى لبطاقة الشبكة، إلا أنه باستطاعتك نقل بطاقة الشبكة من جهاز لآخر أو من شبكة إلى شبكة أخرى وتشغيلها بطريقة عادية .

رمز الشركة المصنعة — رمز بطاقة الشبكة

00 - 06 - 89 - 0B - E1 - 35

3 Bytes — 3 Bytes

شكل ٥-٢ تنسيق العنوان المادي

تقنية Token Ring وFDDI

دفعت مشكلة النزاع علي تردد النطاق الذي يعد جزءاً لا يتجزأ من Ethernet كل من IBM و IEEE إلي ابتكار مقياس ربط شبكات آخر . أطلق عليه IEE 802.5 . ينتمي IEE 802.5 بصورة أكبر إلي Token Ring .

بدأت شركة IBM بترويج مقياس Token Ring الذى اصبح مقياس IEEE 802.5 . ومن هنا جاءت تسميته فى البداية DIX Ethernet. تفوقت سرعه "توكن رينج" فى السنوات الأولى على سرعة مقياس"ايثرنت" ووصلت إلى ١٦ميجابت/ثانية مقابل ١٠ميجابت/ثانية. مما وضع "توكن رنج" فى مرتبة أعلى من مرتبة "ايثرنت". وتميز "توكن رنج" بالإضافة إلى السرعة بميزات أخرى منها قدرته على توصيل أجهزة كمبيوتر شخصية (PCs) وأجهزة كمبيوتر متوسطة (Mini Computers) وأجهزة كمبيوتر عملاقة (Main Frames). وزاد من شهرة "توكن رنج" اسم IBM من ورائه. إلا أن تكلفته ظلت أعلى من تكلفة "اثيرنت" بثلاثة أو خمسة إضعاف.

إلا أن التطور الذى حدث لمقياس "ايثرنت" أزاح "توكن رنج" عن عرشه. حيث أصبح 100BaseT متاحاً على مجال واسع وبلغت سرعته ١٠٠ميجابت /ثانية.

وعندما تطور "توكن رنج" وبلغت سرعته ١٠٠ميجابت/ثانية.ظهر"ايثرنت جيجابت" Gigabit Ethernet الذى تضاعفت سرعته ١٠مرات على "توكن رنج" (راجع البند السابق). ولهذا اختفى بريق مقياس "توكن رينج". وأصبح "ايثرنت" هو السائد فى السوق.

أما عن تقنية FDDI (كلمة FDDI اختصار للعبارة Fiber Distributed Data Interface ومعناها "واجهة بيانات ألياف موزعة").

فقد تم تصميمها فى الأصل لكى تستخدم مع كابل ألياف ضوئية كما يظهر من اسمها ولكن التطبيقات الحديثة تستخدم كابل من نوع UTP "الزوج المجدول غير المحمى" من الفئة الخامسة (CAT5).

تتشابه واجهة استخدام FDDI مع Token Ring. تعتبر تقنية FDDI أيضا باهظة التكاليف إذا ماقورنت بمقياس Ethernet 100Base T مما دفع ايثرنت إلى الصدارة فى

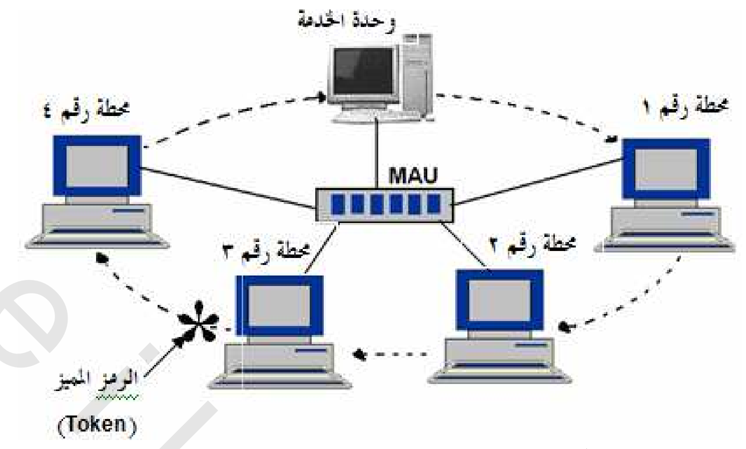
عالم الشبكات. تستخدم **FDDI** أيضا مقياس **802.5** لنقل البيانات علي الشبكة .
يمكن أن يعمل نظام **FDDI** بسرعة ١٠٠ميجابت/ثانية على مسافة إجمالية تبلغ ١٠٠كيلو متر ويمكن أن يستخدم داخل بناية واحدة أو بين البنايات. ويصل طول المقطع إلى ٢كيلومتر وذلك باستخدام ألياف ضوئية.

وسيلة Token Ring و FDDI للتحكم فى تدفق البيانات

يستخدم كل من **Token Ring** و **FDDI** تقنية **802.5** لنقل البيانات على الشبكة. في **Ethernet** يقوم أى جهاز كمبيوتر موجود على مقطع شبكة محدد لنقل البيانات حتى يشعر بتعارض مع جهاز آخر. أما في نظامي **Token Ring** و **FDDI** فالأمر مختلف حيث يتم تكوين حزمة من البيانات يطلق عليها **Token**(رمز مميز) ويتم تمريرها عبر الشبكة. وفى هذه الحالة لا يقوم جهاز الكمبيوتر بنقل حزمة البيانات إلا إذا حصل على الرمز المميز. فإذا تم نقل البيانات، يترك الرمز المميز للشبكة، حيث يتناوله الجهاز التالي لينقل حزمة البيانات الموجودة لديه. وفى التخطيط كما نلاحظ لن تحصل مشكلة التعارض التي تحدثنا عنها في شبكة **Ethernet**. لأن جهاز الكمبيوتر الوحيد الذي يمكنه نقل البيانات هو الجهاز الذي عنده الرمز المميز.

وهذا الرمز المميز عبارة عن رسالة الكترونية يتم تمريرها عبر الشبكة. بعد إتمام النقل يعود الرمز المميز إلى الحلقة حيث يلتقطها جهاز الكمبيوتر الذي يريد نقل حزمة بيانات . وطبعا يعمل **FDDI** بنفس الطريقة. انظر شكل ٥–٣ ومنه تلاحظ أن الجهاز الموجود فى محطة العمل رقم ٣ لديه بيانات لنقلها (أى لديه الرمز المميز) . وهو فقط القادر على النقل. عندما ينتهى من نقل البيانات الموجودة لديه، سوف يعيد الرمز المميز إلى الحلقة، وعندها سوف يلتقطها جهاز الكمبيوتر التالى الذى يحتاج لنقل البيانات. لتقنية **FDDI** حلقتين كاملتين يطلق عليهما الحلقة الأولية (**Primary**) والحلقة الثانوية (**Secondary**) وهما تعملان في اتجاهين متقابلين . يوفر زوجا الحلقات قدراً أساسياً من الوقوع في الأخطاء . فإذا كانت احدي الحلقات مقطوعة ، فستتولى الحلقة الأخرى المهمة . وإذا كان أحد مقاطع الحلقتين مقطوعاً أو إذا لم يعمل أحد الأجهزة أو تمت إزالته ، يمكن ربط الحلقتين

لإعادة تأسيس تكامل الحلقة .



شكل ٥-٣ تدفق البيانات في تقنية Token Ring

يمكننا أن نقول أن كلا من Token Ring و FDDI يعمل بنظام إشـــارات المـــرور. حيث لا تمر السيارة إلا إذا أخذت الضوء الأخضر أما Ethernet فإنها تعمـــل بـــدون إشارات مرور حيث من الممكن أن تتعارض السيارة مع سيارة أخرى قادمة مـــن الاتجـــاه الآخر وهنا يستحيل على أحداهما المرور.

من عيوب Token Ring أنه بطيء ذلك لأنه إذا احتاج أكثر من كمبيوتر لنقل البيانات فى نفس الوقت فإن أجهزة الكمبيوتر ستنتظر حتى يتم نقل بيانات الكمبيوتر الأول وحتى تحصل على الرمز المميز الذي يسمح لها بنقل بياناقما. وأيضا تكلفته عالية، ولهذا السبب فإن Token Ring تنقرض فى الوقت الذى تبقى فيه أجهزة Ethernet على القمة.

***أجهزة* Token Ring**

تنتقل المعلومات فى تقنية Token Ring فى اتجاه واحد فقط فى الكابل، (راجع شكل ٥-٣) حيث تتطلب توصيل نهايات الكابل ببعضهما لتشكيل حلقة، وهذا معناه أن كل جهاز كمبيوتر يجب أن يكون به كابلان ووصلتان، أحدهما وارد والآخر صادر. للتسهيل يـــتم ربط الكابلات، التى يعد كل منها كابلا مزدوجا مجدولا ببعضهما وتستخدم وصلة واحدة. يستخدم "توكن رنج" كابلا مزدوجا مجدولا محمى (STP) وهذا بعكس "ايثرنت" الذى يستخدم كابل مزدوج مجدولا غير محمى.

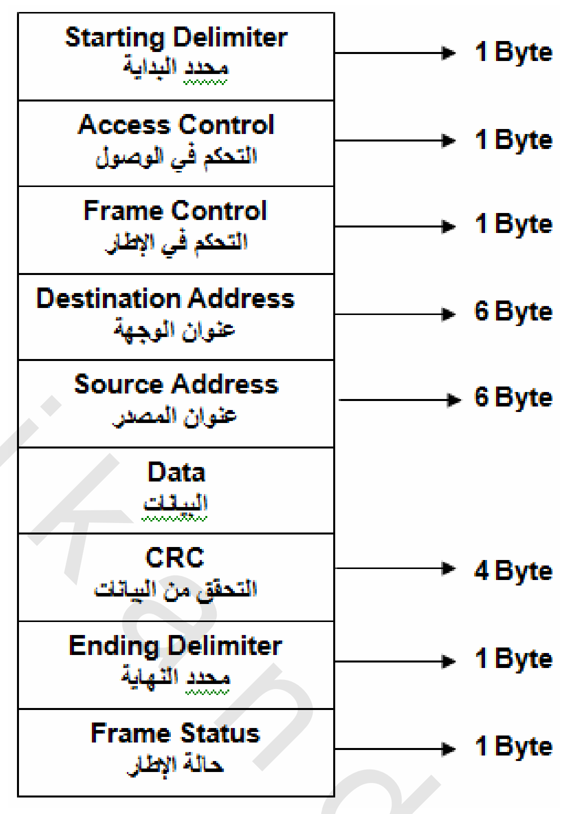
فى شبكات **Token Ring** يتم توصيل كل الأجهزة بواسطة أسلاك إلى نقطة واحدة تدعى **Multistation Access Unit (MAU)** ويمكن ترجمتها وحدة الوصول متعددة المحطات. تشبه **MAU** وحدة التوزيع **(HUB)** أو السويتش المستخدمة فى تخطيط **Ethernet** فى أنها توفر منافذ لتوصيل أجهزة الكمبيوتر ماديا على الشبكة.

كما يتضح من شكل ٥-٤ تنقل **MAU** البيانات من جهاز كمبيوتر إلى آخر فى مسار يكون حلقة. عندما تصل البيانات إلى **MAU** يوجهها إلى المنفذ الذي يليه بدلا من كل المنافذ.

عندما يريد جهاز إرسال بيانات إلى جهاز آخر فإنه يمرر البيانات إلى **MAU** الذي يمررها للجهاز الثانى (التالى فى الحلقة) والذى بدوره يقرأ عنوان الوجهة فى ترويسة الإطار. إذا وجد الجهاز الثانى أن عنوان الوجهة يوافق العنوان المادى المخصص له، يستلم البيانات ويمررها إلى الطبقات العليا. أما إذا كان العنوانان مختلفين، فيمرر الجهاز الثانى البيانات إلى **MAU** الذي يمررها إلى الجهاز الثالث..... وهكذا. إلى أن تصل المعلومات إلى هدفها

***إطار* Token Ring**

يوضح التنسيق التالى تخطيط إطارات "توكن رنج" والحقول التى يشتمل عليها



شكل ٥-٤ نقل MAU البيانات من جهاز إلي جهاز آخر

معظم هذه الحقول موجودة في إطار Ethernet الذي شرحناه قبل قليل ولـــذلك فإننـــا نوضح باختصار هذه الحقول كما يلي :

- **Starting Delimiter**: يستخدم شفرة فريدة للإشارة إلى بداية الإطار.
- **Access control**: يحدد ما إذا كان الإطار علاقة أم لا كما يحدد أولويته.
- **Frame Control**: يشير إلى نوع الإطار وكيفية معالجته.
- **Destination Address**: يحدد عنوان الجهاز المستقبل.
- **Source Address** : يحدد عنوان الجهاز المرسل.
- **Data**: يحتوى على البيانات المطلوب إرسالها.
- **CRC**: يحتوى على رقم يستخدم للتحقق من الإطار (راجع CRC في شرح حقـــول

.(Ethernet

- **Ending Delimiter**: يستخدم شفرة فريدة للإشارة إلى نهاية الإطار.
- **Frame Status**: يخبر الجهاز المرسل أن الإطار قد وصل.

تقنية ATM

كلمة **ATM** اختصار للعبارة **Asymchronous Transfer Mode** ومعناها بالعربية "وضع النقل غير المتزامن" . ولقد جاء تخطيط **ATM** لتلافى عيوب التقنيات الموجودة من قبل والتي شرحناها في البندين السابقين، وهو يعتبر أحدث تقنيات نقل البيانات ومن مميزاته أنه يمكن أن يحمل الصوت والصورة عبر أسلاك الشبكة. من مزايا **ATM** أنه أسرع من غيره حيث يتراوح معدل نقل البيانات بين **٢٥** ميجابت في الثانية و**1.5** جيجابت فى الثانية ولذلك فهو مناسب جدا للتطبيقات التي تتطلب سرعة عالية و خدمة جيدة .ينقل **ATM** كل حزم البيانات بصفتها خلايا تبلغ **٥٣** بايت لها مجموعة متنوعة من المعرفات لتحديد أمور معينة مثل **Quality of Service**"جودة الخدمة".

تقنيات ربط شبكات المنازل

نقصد بشبكات المنازل الشبكات المنزلية والمكاتب الصغيرة مثل مكتب الطبيب والمحامى حيث تمتد الشبكة لمسافة قصيرة داخل شقة مثلاً وتربط عدداً محدوداً من أجهزة الكمبيوتر. فى الشبكات الصغيرة المستخدمة فى المنازل لا يلزمك تركيب كابلات شبكة اتصال منفصلة، إذ بإمكانك استخدام كابلات الكهرباء وكابلات الهاتف التى تستخدمها فى المنزل أو المكتب.

استخدام خط الهاتف فى الشبكة.

ببساطة شديدة يتم توصيل شبكات الاتصال التى تستخدم خطوط الهاتف بمقابس الهاتف المركبة بالفعل فى الحائط بالمنزل. وتنتقل بيانات الشبكة عبر ترددات لاتتداخل مع الاتصالات الصوتية، بحيث يمكن استخدام الشبكة أثناء إجراء المكالمات الهاتفية.

قامت مجموعة **Home Phone line Networking Alliance (HPNA)** بتطوير

إصدارين من المقاييس للشبكات المنزلية. الأول هو إصدار **HPNA 1.0** ويعمل بسرعة تبلغ ١ميجابت/ثانية. والثاني إصدار **HPNA 2.0** ويعمل بسرعة تبلغ ١٠ ميجابت/ثانية. وهو المعدل القياسي لنقل البيانات. يسمح مقياس **HPNA 2.0** بتشبيك عدد من الأجهزة يصل إلى ٢٥ جهازا بمسافة تصل إلى ٣٦٠ مترا بين أى جهازين ومالا يزيد عن ٣٦٠٠ متر مربع من اجمالى المساحة التى يتم تغطيتها.

حتى تتمكن أجهزة الشبكة من رؤية بعضها البعض، يجب توصيل بطاقة شبكة خاصة بالكمبيوتر، ويتم توصيل موائم **USB** بمنفذ **USB** بالكمبيوتر من جانب وبمنفذ الهاتف من الجانب الآخر. وفى هذه الحالة لن تحتاج إلى وحدة توصيل **hub** أو سويتش. كل ما ستحتاجه من أجهزة للشبكة التى تستخدم خطوط الهاتف هو بطاقات الشبكة وموائمات **USB** وكابلات بين منفذ الهاتف وجهاز الكمبيوتر.

معظم المنازل بها زوجين أو أربعة من الأسلاك التى تمر فى إنحاء المنزل حتى يمكن لأى مقبس فى المنزل الوصول إلى أى خط من الخطوط . يسمح هذا الوضع لشبكات الهاتف بالعمل فى أى مكان فى المنزل. لهذا قلنا عن هذه الشبكات "شبكات منزلية".

بروتوكول PPP

PPP اختصار للعبارة **Point-to-Point** ويمكن ترجمتها بروتوكول نقطة إلى نقطة. يستخدم هذا البروتوكول أساساً للتحكم فى نقل البيانات عبر خطوط الهاتف وإدارالها ويستخدم لتوصيل الأجهزة التى لاتوجد بها بطاقة شبكة من خلال شبكة. في كثير من الحالات يستخدم هذا البروتوكول حين تدخل إلي الانترنت من خلال أحد مزودي خدمة الانترنت (**ISP**) . ولذلك يعد **PPP** أحد مقاييس الإنترنت .

لكى تفهم بروتوكول **PPP** يجب أن تعلم أنه يتطلب معرفة الآتى:

- رقم هاتف النظام الذى سيتصل به.
- عنوان **DNS** أو **Domain Name Address** "عنوان اسم النطاق" حيث توفر خادمات **DNS** جدول بحث يبحث فيه جهاز الكمبيوتر ليتمكن من تخصيص عنوان **IP** رقمى لاسم. مثلا يمكن تخصيص عنوان **IP** رقمى مثل **192.168.207.124** لاسم مثل

.compuscience.com.eg

- إذا كان جهاز الكمبيوتر سوف يتصل بالإنترنت، فإنه يحتاج إلى إعداد مدخل افتراضى (عنوان IP للموجه أو المدخل الذى يتصل بالإنترنت). فى تطبيقات PPP، يمكنك إخبار جهاز المستخدم بالحصول على هذه المعلومات من الخادم الذى يتصل به.
- عندما يكون لديك مجموعة محدودة من عناوين IP (سواء كانت عناوين ثابتة أم تم تخصيصها بواسطة الخادم) مثلا ٢٥٥ عنوان ومجموعة كبيرة من المستخدمين مثلا ٥٠ مستخدم يتنافسون على ٢٥٥ عنوان يتم استخدام Dynamic Host configuration Protocol (DHCP) " بروتوكول توصيف المضيف الديناميكى".

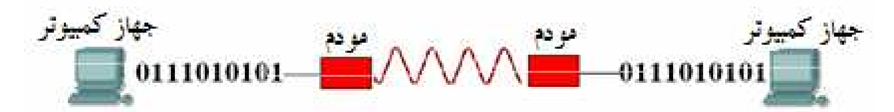
يقوم DHCP بتعيين عناوين IP على حسب الضرورة، وعندما لايتم استخدامها، تعود العناوين إلى المجموعة العامة التى تم سحبها منها.

يعتبر تعيين هذه المتطلبات "المعلَّمات" جزءا من خاصية Dial – up network "اتصال شبكى هاتفى" وهى سمة موجودة فى جميع إصدارات Windows.

آلية عمل PPP

يمكن تلخيص آلية عمل PPP علي النحو التالي :

- يقوم المستخدم بإدخال البيانات إلي جهاز الكمبيوتر الذي يمررها إلي المودم المتصل بالكمبيوتر . تمر البيانات في صورة ثنائية (Bits) يعني خانات من الآحاد والأصفار .
- يقوم المودم بتشفير البيانات الرقمية إلي صوت يمكن أن ينتقل عبر خط الهاتف .
- يمر الصوت بخط الهاتف حتي يصل إلي المودم الموجود علي الطرف الآخر
- يفك المودم الموجود علي الطرف الآخر من الاتصال تشفير الصوت ويحوله إلي بيانات رقمية (Bits) مرة أخري لجهاز الكمبيوتر
- تصل البيانات إلي الجهاز الموجود علي الطرف الآخر الذي يتعامل معها أو قد يمررها إلي شبكة محلية .



ملخص الفصل

شرحنا في هذا الفصل تقنيات الشبكات المحلية ثم شرحنا مقياس **CSMA / CD** كوسيلة للتحكم في تدفق البيانات . ثم شرحنا شبكات **Ethernet** وأوضحنا الفرق بينها وشرحنا أيضا أطر **Ethernet** .شرحنا بعد ذلك تقنية **Token Ring** و **FDDI** وأوضحنا وسيلة **Token Ring** للتحكم في البيانات وشرحنا أيضا أجهزة و أطر **Token Ring** . شرحنا أيضا تقنية **ATM** وتقنيات ربط شبكات المنازل التي تستخدم خطوط الهاتف بالمنازل وتحدثنا عن بروتوكول **PPP** .

تدريبات

١. صل العبارة الصحيحة والتي تحدد المصطلحات والمعاني التي تخص كل تقنية أو مقياس فيما يلي

أ. **Ethernet**	١. تمكين الجهاز الحاصل على العلامة **(Token)** من إرسال بياناته .
ب. **Token Ring**	٢. وسيلة تصف كيفية مشاركة أكثر من جهاز كمبيوتر لقناة ايثرنت واحدة .
ج. **CSMA/CD**	٣. تعتبر أحدث تقنيات نقل البيانات ومن مميزاتها أنها تحمل الصوت والصورة عبر أسلاك الشبكة بالإضافة إلى سرعتها العالية .
د. **ATM**	٤. تشير هذه التقنية إلى أحد نوعي كابلات الهاتف أو كابلات الكهرباء الموجودة بالمنازل ويتم توصيل الشبكات التي تستخدم خطوط الهاتف في مقياس الهاتف الموجودة بالفعل في المنازل .
هـ. ربط الشبكات المنزلية	٥. تعتبر هي التقنية السائدة للشبكات المحلية على نطاق واسع لأنه رخيص نسبياً ويسهل توسيعه وتستخدمه العديد من نظم الكمبيوتر .

٢. صل العبارة الصحيحة والتي تحدد السرعة ونوع الكابل الذي يخص تقنية الشبكة

أ.	10 Base 2	١.	أقصى سرعة ١٠٠٠ / ميجابت / ثانية وتستخدم كابل من نوع ألياف بصرية .
ب.	10 Base T	٢.	أقصى سرعة ١٠ ميجابت / ثانية وتستخدم كابل من نوع محوري رفيع .
ج.	10 Base F	٣.	أقصى سرعة ١٠٠ ميجابت / ثانية وتستخدم كابل من نوع UTP – CAT5 .
د.	100 Base T	٤.	أقصى سرعة ١٠ ميجابت / ثانية وتستخدم كابل UTP – CAT3 .
هـ.	100 Base F	٥.	أقصى سرعة ١٠٠٠ ميجابت / ثانية وتستخدم كابل UTP – CAT5
و.	1000 Base T	٦.	أقصى سرعة ١٠ ميجابت / ثانية وتستخدم كابل ألياف بصرية .
ز.	1000 Base F	٧.	أقصى سرعة ١٠٠ ميجابت / ثانية وتستخدم ألياف بصرية

٣. في أسماء IEEE الخاصة بمقياس أجهزة: Ethernet:

أ. يشير الرقم مثل ١٠ أو ١٠٠ إلى السرعة بالميجابت

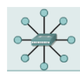
ب. يشير Base إلى Base Band (التردد الأساسي)

ج. يشير T (في الأنواع الحديثة) إلى نوع الكابل UTP

د. يشير الرقم في نهاية المقياس (في الأنواع القديمة) مثل 2 أو 5 مثل 10 Base إلى الحد الأقصى لطول المقطع بالمائة متر

هـ. كل ما سبق

و . لا شئ مما سبق





نموذج OSI عبارة عن نموذج تم تطويره من قبل منظمة ISO الدولية وهو باختصار نموذج لوصف مهمة ربط الشبكات . فهم هذا النموذج سيساعدك في فهم كل من ربط الأجهزة وبروتوكولات الشبكة .

بانتهاء هذا الفصل ستتعرف على :

- ***طبقات OSI السبعة***
- ***مهمة ربط الشبكات***
- ***نقل البيانات في نموذج OSI***

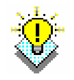
OSI اختصار لعبارة **Open System Interconnection** ومعناها " الاتصال الداخلي للنظم المفتوحة " وقد تم تصميم هذا النموذج بناء على طلب الهيئة العالمية للمقاييس (**International Standard Organization ISO**) وكان الهدف منه هو إيجاد معيار قياس عالمى لتوحيد البروتوكولات المستخدمة في الطبقات المختلفة للشبكة . لقد كان الهدف من هذا النموذج هو إرغام الشركات المتخصصة في الشبكات بإتباع هذا النموذج في تصميمهم حتي تسمح للأنظمة المفتوحة وهي التي لا تنتمي إلي شركة متخصصة في الشبكات بالاتصال والتوافق فيما بينها . وكان الشائع قبل تطوير هذا النموذج إرغام المستخدمين علي التعامل مع أجهزة تابعة لشركات متخصصة في هذا المجال فقط .

مهمة ربط الشبكات

وقبل أن نشرح نموذج **OSI** والطبقات التى يشتمل عليها نشرح فيما يلى مهمة ربط الشبكات ليسهل عليك فهم طبقات نموذج **OSI** وطريقة عملها. تشتمل مهمة ربط الشبكات على العناصر الآتية:

١. تعريف كل كمبيوتر موجود فى شبكة الاتصالات.
٢. تحديد المعلومات المطلوب نقلها كرسالة مستقلة.
٣. إضافة عنوان أجهزة الكمبيوتر المرسلة والمستقبلة لكل رسالة وتمييز كل رسالة بعلامة مميزة.
٤. تضمين الرسالة داخل حزمة بيانات واحدة كما يحصل عندما تضع الرسالة داخل مظروف ليتم نقل المظروف بمحتوياته بواسطة البريد) ويجب أن تشمل حزمة البيانات على عناوين الإرسال والاستلام. والمكان الذى تنتمى إليه حزمة البيانات داخل الرسالة.
٥. وضع حزمة البيانات داخل إطارات **Frames** يتم نقلها عبر الشبكة
٦. مراقبة تدفق الاتصالات على الشبكة لمعرفة التوقيت المناسب لإرسال إطار لتجنب التصادم مع إطارات أخرى قد تكون مرسلة فى نفس اللحظة على الشبكة .

٧. عند التأكد من خلو الاتصالات على الشبكة يتم نقل الإطار اعتماداً على أجهزة الربط المستخدمة.
٨. توفير الوسائل المادية التى تلزم لنقل الإطارات بين الأجهزة مثل الأسلاك والبطاقات.
٩. مراقبة تدفق الاتصالات على الشبكة لمعرفة متى يتم استلام الإطار.
١٠. استلام الإطار الموجود على الشبكة.
١١. استخراج حزمة البيانات الموجودة فى إطار واحد أو أكثر ومزجها فى الرسالة الأصلية.
١٢. تحديد ما إذا كانت الرسالة تخص الكمبيوتر المستلم لتتم معالجتها أو لا تخصه فيتم تجاهلها.



يتم استخدام أسماء مختلفة وأحيانا محيرة للإشارة إلى أجزاء من البيانات يتم نقلها عبر شبكة اتصال من هذه الأسماء الرسائل وحزم البيانات والإطارات. فى الفصول التالية ستجد توضيحا أكثر لهذه الأسماء.

لوصف مهمة ربط الشبكات بصورة أفضل قامت منظمة OSI الدولية بتطوير نموذج OSI وعن هذا النموذج نوضح ما يلى:

- نموذج OSI بحد ذاته ليس بنية شبكية ، لأنه لا يحدد الخدمات والبروتوكولات الواجب استخدامها مع كل طبقة بل يحدد فقط وظيفة كل طبقة من الطبقات، وقد ينتج عن هذه البنية مجموعة من المعايير تخص كل طبقة من البنية، ولا تعتبر هذه المعايير جزءا من النموذج، وإنما تم نشرها كمعايير عامة منفصلة عن توصيف نموذج OSI.
- يعد نموذج OSI صورة نظرية لكيفية تحرك البيانات في الشبكة.
- نموذج OSI ليس ملموسا وهو لا يؤدى أي وظيفة في عمليات الاتصالات. العمل الفعلي يتم بواسطة البرامج والأجهزة .
- نموذج OSI يعرف أي الأعمال يجب أن تتم وأى البرتوكولات ستتناول تلك الأعمال عند أي من الطبقات السبعة للنموذج.

طبقات نموذج OSI

يشمل الشكل (٦- ١) على رسم تخطيطي لنموذج **OSI** ومنه نلاحظ أن هذا النمــوذج يشتمل على ٧طبقات أو(شرائح) تأخذ الأرقام من ١إلى٧ وتتلخص المبادئ التي اعتمدت للوصول إلى هذا التقسيم فيما يلى :-

١. يجب على كل طبقة أن تنفذ مهام ووظائف محددة ومعرفة بوضوح.مما يــؤدى إلى تقسيم مهمة ربط الشبكات إلى سبع مهام صغيرة.
٢. يجب اختيار الوظائف بحيث تساعد فى تعريف بروتوكولات قياسية عامة .
٣. يجب اختيار حدود الطبقات بحيث تقلل ما أمكن من تدفق البيانات عبر الواجهــات بين الطبقات .
٤. يجب أن يكون عدد الطبقات كافٍ حتى لا نضطر لوضع عدة وظائف مختلفة فى نفس الطبقة إلا عند الضرورة ، كما يجب ألا يزداد عدد الطبقات بحيث تفقد البنية قوتها ومرونتها .

سوف نناقش فيما يلى كل طبقة من طبقات هذا النموذج على حدة ، مبتدئين من الطبقة السفلية .

Layer 7 الطبقة ٧ — Application التطبيق
Layer 6 الطبقة ٦ — Presentation تقديم
Layer 5 الطبقة ٥ — Session جلسة
Layer 4 الطبقة ٤ — Transport نقل
Layer 3 الطبقة ٣ — Network شبكة
Layer 2 الطبقة ٢ — Data Link ربط البيانات
Layer 1 الطبقة ١ — Physical مادية

شكل ٦–١ طبقات نموذج OSI

الطبقة المادية The physical layer

تهتم هذه الطبقة كما هو واضح من اسمها بالمكونات المادية داخل الشبكة مثل الأسلاك والألياف البصرية وأجهزة التوصيل وبطاقات الشبكة . تحدد هذه الطبقة ماهية الجوانب المادية وماذا يمكن أن تفعل عن طريق التحقق من مواصفات الكابلات والمقاييس..... وغيرها.

تهتم الطبقة المادية بإرسال خانات المعلومات عبر قناة الاتصال وتكون المهمة الأساسية عند التصميم هى تقديم الضمانة بوصول المعلومات المرسلة إلى المستقبل دون ضياع أو تشويه، أى أن الخانة التي تحتوي على ١ والمرسلة من أحد الأطراف يجب أن تصل مع احتوائها على نفس القيمة١ إلى الطرف الآخر في حالة الإرسال ، تقوم الطبقة المادية بخدمة طبقة ربط البيانات وهذه الأخيرة تحدد نوع تقنية الشبكة المحلية كتقنية **Ethernet** وتقنية **Token Ring** . في حالة الاستقبال تحول هذه الطبقة النبضات الالكترونية أو الضوئية إلي رموز

ثنائية (**0 , 1**) لمعالجتها بواسطة طبقة ربط البيانات .

إن معظم اعتبارات التصميم هنا تدور حول المفاهيم الميكانيكية والالكترونية وإجـراءات التخاطب والوسط المادى للنقل وهى عبارة عن بطاقة الـشبكة والموصـلات وتوصـيل الكابلات.

طبقة ربط البيانات The Data Link Layer

تحدد طبقة ربط البيانات نوع تقنية الـشبكة المـستخدمة . هـل هـي تقنيـة **Ethernet** أم تقنية **Token Ring** أم تقنية **FDDI** وحسب التقنية المستخدمة يتحـدد نوع أجهزة التوصيل والكابلات وبطاقات الشبكة المطلوب استخدامها .

تنحصر مهمة طبقة ربط البيانات فى استلام البيانات الخام المرسلة مـن الطبقـة الماديـة (طبقة١) كما هى وتحويلها إلى بيانات خالية من أخطاء الإرسال ومن ثم نقلها إلى طبقـة الشبكة (**Network layer**). وتنجز هذه الطبقة مهمتها بجعل المرسل يقوم بتقسيم بيانات الدخل إلى إطارات بيانات (كل منها بحجم عدة مئات أو عدة ألاف من البايتات)، وإرسالها بشكل تسلسلي .

وبما أن الطبقة المادية عادة تقوم بإرسال سلاسل من الخانات بدون أى اعتبـار لمعناهـا أو بنيتها ، فان على طبقة ربط البيانات أن تعيد تشكيل الإطارات وتحديد بداياتها و نهاياتها ، ويمكن أن يتم ذلك بإضافة بعض تشكيلات الخانات الخاصة إلى بداية ونهاية كل إطـار ، بمعني أن طبقة ربط البيانات تضيف ترويسة وتذييل لبيانات طبقة الشبكة ثم تمرر الإطار إلي الطبقة المادية التي تقوم بدورها بإرسال البيانات علي الشبكة . ففي الترويـسة توضـع عناوين **Media Access Control (MAC)** " عناوين التحكم في وصول الوسـائط " للجهازين المرسل والمستقبل . وعنوان **MAC** هو عنوان يبلغ ٦ بايت (**48 Bit**) فريد لكل بطاقة شبكة ويتم تمثيله باستخدام الرموز السداسية العشرية (**HEX.**) . وتجدر الإشارة إلي أن هذا العنوان تم توليده من طرف طبقة الشبكة . ويشير دائماً إلي جهاز كمبيوتر موجود علي نفس الشبكة حتي ولو كان الجهاز النهائي المقصود الوصول إليه موجود علي شـبكة أخري .

إن وجود ضجيج على خط النقل يمكن أن يدمر الإطار بالكامل، وفى هذه الحالة تقوم طبقة ربط البيانات فى طرف المرسل بإعادة إرسال الإطار. وقد يؤدى الإرسال المتعـــدد لـــنفس الإطار إلى مضاعفة المعلومات ويحدث ذلك إذا فقدت إشارة الإعلام بالوصول المرسلة من قبل المستقبل، وعلى طبقة ربط البيانات أن تحل المشاكل الناتجة عن تخريـــب وضـــياع أو مضاعفة الإطارات . كيف ذلك ؟ للكشف عن الأخطاء يؤدي الجهـــاز المرســـل عمليـــة حسابية علي محتوي بيانات رزمة الإطار ، ثم يرسل الناتج في تذييل الإطار . وعند استقباله للبيانات يؤدي الجهاز المستقبل نفس العملية علي محتوي البيانات المـــستقبلة ثم يقـــارن النتيجة المتحصل عليها مع النتيجة المرسلة . إذا كانت قـــيم النتـــائج متـــشابهة ، يقـــوم بروتوكول طبقة ربط البيانات بتمرير المعلومات إلي الطبقة العليا ، وفي حالـــة اخـــتلاف النتائج ، يرسل الجهاز المستقبل رسالة للجهاز المرسل يطلب إعادة إرساله آخر إطار .

تقدم طبقة ربط البيانات عدة أنواع من الخدمات إلى طبقة الشبكة وكل منها يتميز بنوعية مختلفة وكلفة موافقة لهذه النوعية .

طبقة الشبكة The Net work Layer

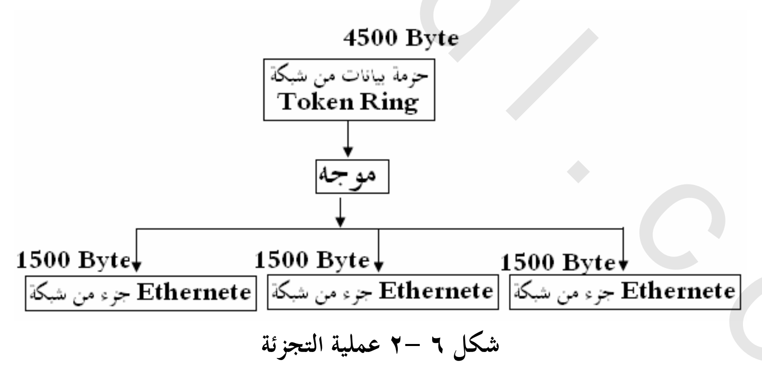
إذا كانت طبقة ربط البيانات تعمل فقط للربط علي نفس الشبكة ، فإن طبقـــة الشبكة يمكنها أن تعمل علي شبكات مختلفة ، وتكون مسئولة عن الاتصالات بين الأجهزة الطرفية حتي لو كانت موجودة علي شبكات مختلفة .

إن مهمة طبقة الشبكة هى التحكم بالبيانات فى مستوى الأجهزة الطرفية ، وتهتم اعتبارات التصميم فى عملية التحكم بتوجيه حزم البيانات من الجهاز المرسل إلى الجهاز المـــستقبل، سواء كانت هذه الأجهزة علي شبكة محلية (LAN) أو شبكة واسعة (WAN) . طبقـــة الشبكة هي المسئولة عن التوجيه (Routing) لتمكين البيانات من الوصول إلي وجهتـــها الأخيرة مهما كان حجم الشبكة . ويمكن أن تعتمد الموجهات (Routers) لأداء هـــذه المهمة على جداول ثابتة ومزروعة داخلها كما يمكن أن يتم بناء وتحديد هذه الجداول عند كل عملية تأسيس اتصال، كما فى حالة اتصال طرفى عبر الشبكة (جلسة عمل على محطة عمل مربوطة مع وحدة خدمة). ومؤخرا أصبحت الموجهات على درجة عالية من المرونـــة

حيث أنها تقوم بإعادة بناء الجدول مع كل حزمة يتم تحريرها وتوجيهها مما يعكس حالة الحمل على الشبكة فى كل لحظة.

وإذا ازدحمت الحزم بحيث ازداد عددها على شبكة فرعية فى لحظة ما، فإن ذلك سوف يؤدى إلى إعاقة إحداها للأخرى ، مما يوصل الخط إلى حالة عنق الزجاجة فى نقطة الازدحام، وحل مثل هذه المشاكل هو من مهام طبقة الشبكة.

وعندما يكون على الحزمة المرور من شبكة فرعية إلى أخرى فإن العديد من المشاكل يمكن أن تظهر ، ، فقد لا تقبل الشبكة الثانية الحزمة بسبب حجمها الكبير الذى لاتستطيع أن تتعامل معه ،فعلي سبيل المثال يبلغ أقصي حجم للحزمة في تقنية **Token Ring** ٤٥٠٠ بايت بينما تبلغ ١٥٠٠بايت في حالة **Ethernet** وهنا يلزم تجزئة المخطط البياني للحزمة (يبين شكل ٦ –٢ عملية التجزئة) وقد تكون البروتوكولات المستخدمة فى كل منهما مختلفة، مثلاً يستخدم تروتوكول **IPX** لشبكات **Netware** بينما يستخدم بروتوكول **NetBeui** لشبكات **Windows** ، من أشهر البروتوكولات المستخدمة لطبقة الشبكة بروتوكول الانترنت (**Internet Protocol**) وحل جميع هذه المشاكل يقع على عاتق طبقة الشبكة التى يجب أن تتجاوزها وتؤمن الاتصال بين شبكتين غير متشابهتين.



شكل ٦ –٢ عملية التجزئة

طبقة النقل **Transport layer**

تعد هذه الطبقة هي المكان الذي يعمل فيه جزء **TCP** من بروتوكول **TCP/IP** . ولذلك فإن طبقة النقل تتمم خدمات طبقة الشبكة .إن الوظيفة الأساسية لطبقة النقل هى

قبول بيانات من طبقة الجلسة وتقسيمها إلى أجزاء صغيرة إذ تطلب الأمر ثم تحريرها إلى طبقة الشبكة، والتأكد من أن كل القطع الصغيرة قد وصلت بشكل صحيح إلى الطرف الآخر.

وإذا تطلبت عملية النقل معدل سرعة أعلى من المتاح، تقوم طبقة النقل بتوليد عدة اتصالات شبكية وتقوم بإرسال البيانات وتقسيمها على جميع الوصلات المولدة بحيث تزيد من سرعة النقل .وعلى طبقة النقل أن تقرر نوع الخدمة التى يجب تقديمها إلى طبقة الجلسة، وأكثر الأمثلة شعبية عن اتصال النقل هى قناة نقطة لنقطة خالية من الأخطاء تقوم بإيصال البايتات والرسائل بالترتيب الذى أرسلت به، Free- error, pear-to-pear channel .وهناك نوع آخر من خدمات النقل هو نقل الرسائل المنفصلة دون أى ضمانة بالوصول بنفس الترتيب.

في الطبقات الأدنى تكون البروتوكولات بين كل جهاز والجهاز المجاور له مباشرة وليس بين الجهاز المصدر والجهاز الهدف مباشرة، والذى يمكن أن يكون بينهما عدة موجهات.

تشتمل طبقة النقل علي نوعين من البروتوكولات ، النوع الأول يقدم خدمات تعتمد علي الاتصال الموجه ومن أمثلتها بروتوكول Transmission Control Protocol (TCP) ومعناه "بروتوكول التحكم في النقل" . وفي هذا البروتوكول يكون تبادل البيانات مسبق بين النظامين لتأسيس اتصال بينهما ، النوع الثاني عديم الاتصال ومن أمثلتها بروتوكول User Datagram Protocol (UDP) وهو نادر الاستخدام ولذلك لن نتوقف عنده . يقدم TCP الخدمات الآتية :

- *تجزئة البيانات Data Segmentation :* عندما يقوم جهاز بإرسال ملف ذو حجم كبير، فإن المستخدم يشكو من بطء الجهاز . وذلك لأن إرسال كمية كبيرة من المعلومات دفعة واحدة يعرض الشبكة لبطء شديد. لأن جهاز واحد هو الذي يستخدم الشبكة والأجهزة الأخرى منتظرة . لذلك فإن عملية تجزئة البيانات تمكن الأجهزة الأخرى من العمل بالتناوب علي الشبكة . حيث أن إرسال جزء صغير من المعلومات يعطي الفرصة لجهاز آخر . تفيد عملية تجزئة البيانات كذلك في حالة الإرسال الخطأ حيث يقوم النظام

المرسل بإعادة عملية الإرسال من جديد عند حدوث خطأ.

- *ترقيم وترتيب الأجزاء المرسلة :* تؤدي عملية تجزئة الملفات إلي احتمال أن تصل هذه الأجزاء بترتيب غير سليم . لأن الرزم تأخذ مسارات مختلفة . يتولي **TCP** عملية ترتيب هذه الأجزاء وتجميعها
- *الإشعار باستلام الرزم* : وبالتالي يتأكد النظام المرسل أن رسائله وصلت بنجاح وبالتالي يتواصل في عملية الإرسال .

طبقة الجلسة The Session Layer

تسمح طبقة الجلسة لمستخدمين يعملان على جهازين يستخدمان كوحدتى خدمة أن يقيما جلسة فيما بينهما أي تسمح بتبادل المعلومات بينهما. وتسمح طبقة الجلسة بتبادل نقل البيانات بين الجهتين كما تفعل طبقة النقل بالإضافة إلى أنها تقدم بعض الخدمات المتقدمة التى تحتاجها بعض التطبيقات.

من الأساليب الشائعة في أي عملية اتصالات نظام **Two Way Simultaneous** ومعناه التزامن ثنائي الاتجاه وهو يسمح بنقل الملفات باتجاهين في نفس الوقت يعني يعمل الجهاز المرسل والمستقبل في نفس الوقت يسمي هذا الأسلوب أيضاً **Full Duplex** . وإذا كانت خطوط النقل لا تسمح بالحركة إلا باتجاه واحد فإن طبقة الجلسة تقوم بتحديد الأدوار والسماح باستعمال خط النقل لجهة واحدة فى وقت واحد. يعني من الجهاز الأول إلي الجهاز الثاني أو من الثاني إلي الأول ولكن لا يسمح سوي لجهاز واحد أن يرسل في نفس الوقت أما الجهاز الثاني فسيكون في حالة استقبال فقط . يسمي هذا الأسلوب **Two Way Alternate** أو **Half Duplex** ومعناه التناوب ثنائي الاتجاه .

وإحدى الخدمات المرتبطة بهذه الطبقة هى إدارة العلامة **Token Management**، فمن أجل بعض البروتوكولات لا يمكن لطرفيتين أن تقوما بعملية حرجة فى نفس الوقت، ولتجنب التضارب المحتمل تقوم طبقة الجلسة بتقديم علامة**(Token)** . يقوم المتحاورون بتبادلها فيما بينهم للمساعدة فى تنظيم الدور، ويسمح للطرف الذى يملك العلامة فقط أن يقوم بالعملية الحرجة، حيث يقدمه للتالى بعد أن يفرغ من عمليته .

وتعتبر خدمة التزامن **Synchronization Service** نوع آخر من خدمات طبقة الجلسة، ولفهم هذه الخدمة دعونا نتخيل أننا نريد نقل ملف بين جهازين متصلين وأن عملية النقل تستغرق ساعتين، علما أن الفاصل المتوقع بين انهيارين متتاليين لأحد الأنظمة على الجهازين هو ساعة ونصف، فى هذه الحالة كلما حدث الانهيار أثناء عملية النقل سوف يقوم النظام بإعادة العملية من البداية وطبعا سوف تنهار بعد مرور ساعة ونصف. وهكذا فإن النظام لن يتمكن من إنهاء العملية مطلقا ، هنا يأتي دور طبقة الجلسة فى حل هذه المشكلة بحيث أنها تحشر نقاط اختبار ضمن سلسلة البيانات المنقولة تدعى **check points**، وعند انهيار النظام يكفى إعادة العمليات ابتداءً من آخر نقطة اختبار فقط، أى لا يتم إعادة نقل البيانات التى تقع قبل نقطة الاختبار الأخيرة، وبهذه الطريقة يمكن تجاوز الانهيار ونقل كامل الملف.

طبقة التقديم The Presentation Layer

وظيفة طبقة التقديم هي تمكين جهازي كمبيوتر مختلفين من الاتصال أو التفاهم فيما بينهما يجب تمثيل هذه البيانات بشكل موحد ومجرد ومعيارى حيث يتم نقل البيانات بهذا الشكل عبر خط النقل بين الجهازين وتقوم طبقة التقديم بإدارة هذه العملية حيث تحول المعلومات المرسلة على الشبكة إلى الترميز الموحد ، ومن الأمثلة علي ذلك عملية الترميز **Coding** لأي حرف مثلاً بمقابله في شفرة **ASCII** وعملية ضغط البيانات (**Data Compression**) التي تسمح بتخفيض حجم البيانات المرسلة علي الشبكة مما يسبب سرعة نقل البيانات علي الشبكة . وعملية تشفير البيانات (**Data Encryption**) وهي آلية لحماية البيانات المرسلة علي الشبكة عن طريق تشفيرها باستخدام مفتاح يعرفه الجهاز المستقبل ثم تقوم بتفسيرها أو تقديمها إلى الجهاز في الطرف الآخر، وبالشكل الذي يستطيع أن يفهمه حيث يتم فك الضغط وفك التشفير وترجمة رموز **ASCII** إلي حروف يستطيع المستخدم التعامل معها .

طبقة التطبيق The Application layer

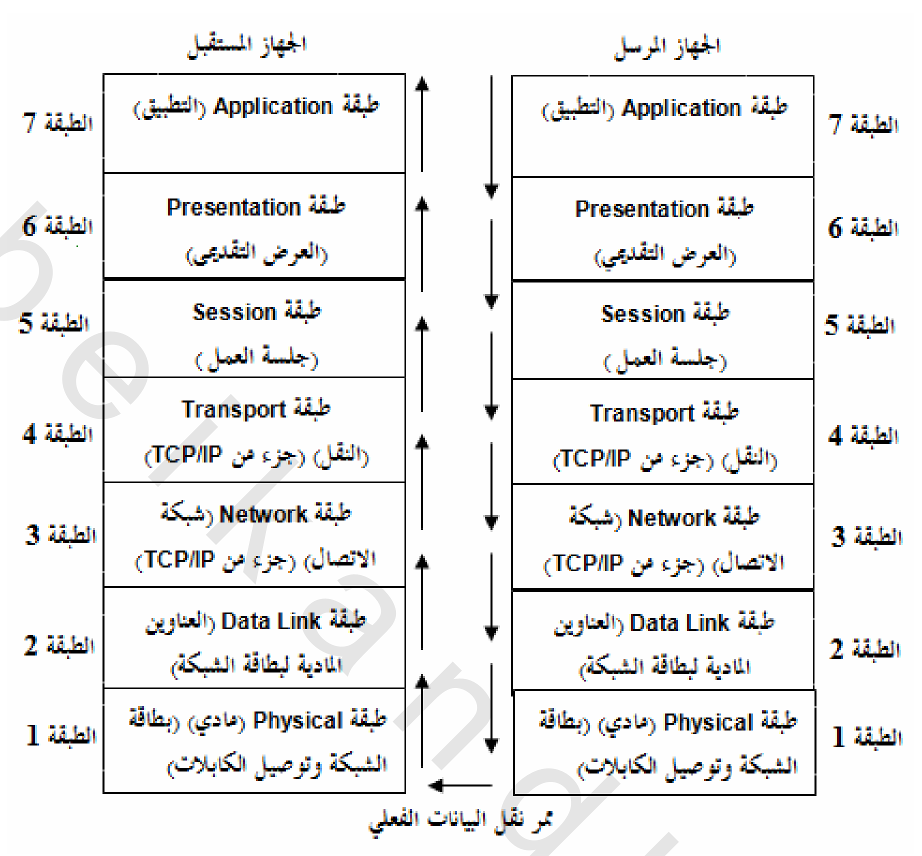
تحوى طبقة التطبيقات على أنواع البروتوكولات التى يحتاجها الجهازين للاتصال فيما بينهما، فمثلا هناك مئات الأنواع من الشاشات الطرفية فى العالم والغير متوافقة غالبا، ولنتصور الورطة التي يمكن أن يقع فيها برنامج تحرير نصوص موجود على وحدة الخدمة وعليه أن يتعامل مع مجموعة من الشاشات الطرفية **Terminals** المختلفة الأنواع وكل منها لها نمط إخراج مختلف للنص وطريقة تحريك مختلفة للمؤشر .

إن الطريقة الوحيدة لحل هذه المشاكل هي استخدام تطبيقات البرامج التي تستخدمها علي الشاشة. وتعتبر عملية نقل وتبادل الملفات مهمة أخرى من مهام هذه الطبقة، فأنظمة الملفات المختلفة لديها اصطلاحات وقواعد مختلفة لتسمية الملفات أو لتمثيل الأسطر النصية فى ملف مثلا. ومن أجل تحقيق عملية نقل صحيحة يجب أولا معالجة عدم التوافقية هذه والعديد من الأمور الأخرى التى يعود أمر معالجتها إلى طبقة التطبيق مثل بروتوكول نقل البريد البسيط **Simple Mail Transfer Protocol(SMTP)** الذي يستخدم في معالجة برامج البريد الإلكتروني (**e-mail**) ، وبروتوكول نقل الملفات (**FTP**) ، وعمليات الدخول عن بعد إلى الشبكة (**Telnet**) وغيرها.

كيفية تحرك البيانات في الشبكة

يوضح شكل (٦–٣) كيف تتحرك البيانات في الشبكة باستخدام نموذج **OSI** وتتم كما يلي .

١. تتجه البيانات إلي أسفل من خلال طبقات **OSI** علي جهاز الكمبيوتر المرسل
٢. بعد معالجة البيانات علي الجهاز المرسل ، تعبر البيانات الشبكة عبر الوسيط المادي (الكابلات)
٣. تتجه البيانات إلي أعلي من خلال طبقات **OSI** علي جهاز الكمبيوتر المستلم



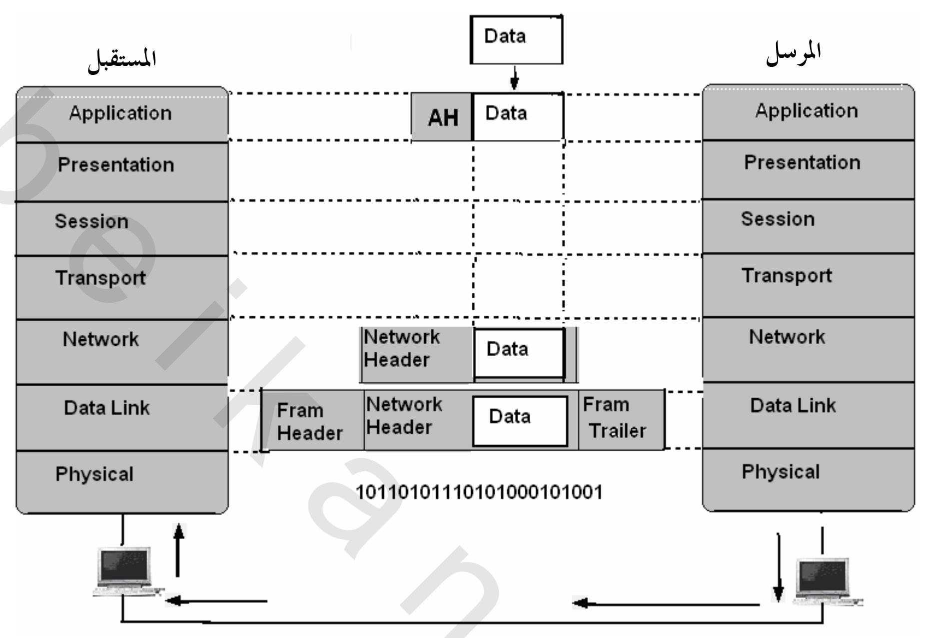
شكل ٦–٣ كيفية تحرك البيانات في الشبكة

نقل البيانات فى نموذج OSI

يظهر من الشكل ٦–٤ طريقة نقل البيانات باستخدام نموذج **OSI** ، فالجهاز المرسل لديه بعض البيانات التى يريد إرسالها إلى الجهاز المستقبل ويقوم المرسل بتسليم البيانات إلى طبقة التطبيق التى تضيف إليها ترويسة التطبيق **Application Header** **(AH)** والذى يمكن أن يكون فارغا حيث تضعها فى مقدمة رزمة البيانات ثم تسلمها إلى طبقة التقديم .

يمكن لطبقة التقديم أن تمرر الرزمة المستلمة بعدة أشكال ويمكن أن تضع فى مقدمتها ترويسة أولا تفعل، وتعطى الناتج إلى طبقة الجلسة، ويجب أن نتذكر أن طبقة التقديم لا تهتم

بتحديد أى جزء من البيانات المسلمة لها من طبقة التطبيق هي ترويسة (إن وجـــدت) أو بيانات حقيقية .



الشكل ٦–٤ نقل البيانات في نموذج OSI

ويتكرر هذا الإجراء حتى تصل البيانات إلى الطبقة المادية حيث يتم إرسالها فعليا إلى الجهاز المستقبل، في الاستقبال تحدث العملية العكسية حيث يتم حـــذف الترويـــسات المرافقـــة للبيانات الواحدة تلو الأخرى، كلما انتقلت الرسالة إلى طبقة أعلى حتى تصل أخـــيرا إلى الجهاز المستقبل .

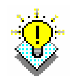
إن الفكرة الرئيسية هنا هى أنه بالرغم من أن المسار الفعلى للبيانات هو بشكل عمـــودى عبر الطبقات فى كل جهاز كما يبين الشكل ٦–٥ فإن كل طبقة قد تمت برمجتها وكأنهـــا تتخاطب مع الطبقة المقابلة لها بشكل أفقي. (انظر شكل ٦–٥) .

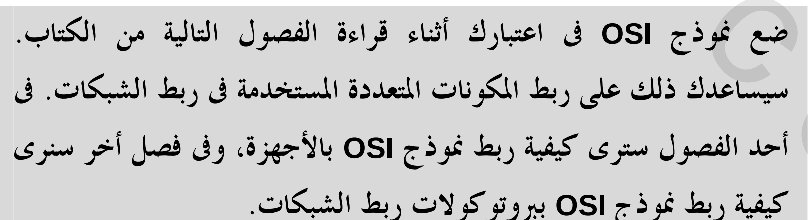
مثلا عندما تستلم طبقة النقل فى جهة المرسل الرسالة من طبقة الجلسة فإنها تضيف إليهـــا ترويسة النقل وترسلها إلى طبقة النقل فى جهة المستقبل، ومن وجهة نظرها فإن ضـــرورة تمريرها إلى طبقة الشبكة فى جهازها أمراً غير ذو أهمية وتعتبره طريقة لإيصال الرسالة فقط،

فمثلا عندما يتحدث دبلوماسى فى اجتماع لهيئة الأمم المتحدة فإنه يوجه كلامه (بلغته الخاصة) إلى بقية الأعضاء مباشرة، ولا تعتبر قضية وجود المترجم الذى يقوم بترجمة كلامه إلى الآخرين أمرا يجب أن يهتم به، ويعتبر هذا الأمر تفاصيل تقنية يفترض ألا تغير من محتوى خطابه .



شكل ٦–٥ قناة افتراضية بين كل قناة ونظيرتها





ضع نموذج OSI فى اعتبارك أثناء قراءة الفصول التالية من الكتاب. سيساعدك ذلك على ربط المكونات المتعددة المستخدمة فى ربط الشبكات. فى أحد الفصول سترى كيفية ربط نموذج OSI بالأجهزة، وفى فصل أخر سنرى كيفية ربط نموذج OSI ببروتوكولات ربط الشبكات.

ملخص الفصل

بدأنا في هذا الفصل بشرح مهمة ربط الشبكات ليسهل عليك فهم طبقات نموذج OSI ووظيفة كل منها . شرحنا بعد ذلك بالتفصيل كل طبقة من طبقات نموذج OSI السبعة

والوظيفة التي تؤديها ، شرحنا ايضاً كيفية تحرك البيانات في الشبكة. وأخيرا شرحنا نقل البيانات في نموذج OSI

تدريبات

1. **في نموذج OSI طبقة ربط البيانات هي الطبقة رقم:**

(٢ ـــ ٥ ـــ ١ ـــ ٤)

2. **رتب طبقات OSI السبعة:**

(الشبكة ـــ التطبيق ـــ المادية ـــ ربط البيانات ـــ الجلسة ـــ تقديم ـــ النقل)

3. **صل الإجابة الصحيحة فيما يلي والتي تحدد المصطلحات والوظائف التي تخص كل طبقة من طبقات نموذج OSI**

الطبقة	الوصف
أ. الشبكة	١. ضغط البيانات Compression وتشفيرها Encryption
ب. المادية	٢. تقوم بتجزئة البيانات (Data Segmentation) إلي أجزاء صغيرة ثم تحريرها إلي طبقة الشبكة . تستخدم بروتوكول TCP و UTP
ج. النقل	٣. يمكنها أن تعمل على شبكات مختلفة وهي المسئولة عن التوجيه . تستخدم بروتوكول IP
د. الجلسة	٤. تتسلم البيانات الخام من الطبقة المادية، وتقوم بإرسال البيانات إلى طبقة الشبكة بعد وضعها في إطارات Frames
هـ. التطبيق	٥. في حالة الاستقبال تقوم بتحويل إطارات طبقة ربط البيانات إلى رموز ثنائية (1,0). وفي حالة الإرسال تقوم بخدمة طبقة ربط البيانات عن

طريق إرسال خانات المعلومات دون ضياع أو تشويش

و. التقديم — ٦. تسمح لمستخدمين يعملان مع جهازي وحدة خدمة أن يقيما جلسة أو حوار بينهما. وتقوم بتحديد الأدوار والسماح باستعمال خط النقل لجهة واحدة في وقت واحد (التناوب ثنائي الاتجاه) . أو تمكين جهازين من الإرسال والاستقبال في نفس الوقت (التزامن ثنائي الاتجاه)

ز. ربط البيانات — ٧. تقوم بمعالجة عدم التوافق بين الأجهزة عن طريق استخدام تطبيقات البرامج المختلفة والبروتوكولات مثل بروتوكول **TCP** وبروتوكول **SMTP**

٤. طورت منظمة **ISO** العالمية نموذج **OSI** المرجعي لغرض:

أ. تزويد المستخدمين بطريقة وصول سريعة إلى خدمات الشبكة

ب. وضع طريقة مناسبة لتشغيل الكمبيوترات

ج. وضع لغة برمجة قياسية لجميع الكمبيوترات

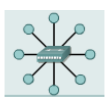
د. تمكين منتجي شبكات الكمبيوترات من التعامل مع بعضهم البعض

٥. أي العبارات التالية تصف طريقة نقل البيانات في نموذج **OSI**:

أ. يقوم الجهاز المرسل بإرسال البيانات إلى طبقة التطبيق التي تمر مباشرة إلى الطبقة المادية ومنها إلي الجهاز المستقبل

ب. تمر البيانات من الجهاز المرسل إلى الجهاز المستقبل مباشرة دون حاجة لوجود طبقات

ج. يقوم الجهاز المرسل بتسليم البيانات إلى طبقة التطبيق التي تضيف أو لا تضيف إليها ترويسه التطبيق ، ثم تسلمها إلى طبقة التقديم. يمكن لطبقة التقديم أن تضيف إليها ترويسه أو لا تضيف وتعطي النتائج إلى طبقة الجلسة ويتكرر هذا الإجراء حتى تصل البيانات إلى الطبقة المادية حيث يتم إرسالها إلى الجهاز المستقبل.





*شرحنا في الفصل السابق النموذج المرجعي للاتصال بين الأجهزة **OSI** وفي هذا الفصل نتناول نموذجاً هاماً وهو نموذج **TCP/IP** . يعمل هذا البروتوكول علي نقل البيانات من وإلي أجهزة الكمبيوتر عبر شبكة الانترنت . بانتهاء هذا الفصل ستتعرف علي :*

- *ما هو المقصود ببروتوكول **TCP/IP***
- *طبقات نموذج **TCP/IP***
- *عناوين **IP***
- *مقارنة بين النموذج **OSI** والنموذج **TCP/IP***
- *عيوب النموذج **TCP/IP***

مقدمة إلي بروتوكول TCP/IP

كلمة **TCP/IP**مأخوذة من العبارة **Transmission Control Protocol/Internet Protocol** ومعناها (بروتوكول التحكم في الإرسال / بروتوكول الانترنت) ويعد هذا البروتوكول واحداً من أهم وأشهر بروتوكولات الشبكة، لأنه مقياس مفتوح لا تتحكم فيه أي شركة فهو أحد المقاييس التي أنشأهَا هيئة عالمية تسمي **IETF** أي **Internet Engineering Task Force** ويمكن ترجمتها هكذا (قوة هندسة الانترنت). وقد جاءت شهرة بروتوكول **TCP/IP** لأنه هو البرتوكول الذى يحمل تدفق البيانات عبر الانترنت.

تقوم لجان معينة بوضع مقاييس **IETF** ويتم تقديمها إلي جماعة ربط الشبكات من خلال مجموعة مستندات تسمي**"RFCS"(Requests For Comments)** يعمل هذا البرتوكول علي نقل البيانات من وإلي أجهزة الكمبيوتر عبر شبكة الانترنت . لا يلزمك سوى التأكد من أن هذا البروتوكول قد تم تهيئته بصورة صحيحة علي كل جهاز كمبيوتر متصل بالشبكة حتي تتمكن جميع الأجهزة من الاتصال بالإنترنت .

يعمل هذا البروتوكول في مستوي أدني من نموذج **OSI** حيث يشكل **TCP** طبقة النقل (**Transport**) وهي الطبقة رقم ٤ في نموذج **OSI** التي تنظم تدفق البيانات، وتشكل **IP** طبقة شبكة الاتصال (**Network**) في النموذج **OSI** وهي الطبقة رقم ٣ التي تتعامل مع العنونة .

ومن الأمور التي يجب أن تعرفها عن بروتوكول **TCP / IP** ما يلي :

- يعمل مع جميع البرامج والأجهزة بغض النظر عن الشركات المنتجة لها.
- يستخدم بروتوكول **TCP/IP** أي نوع من الكابلات ولذلك لا يلزمك تغيير الكابلات التي قمت بتبديلها عندما تريد استخدامه.
- يعمل بروتوكول **TCP/IP** بتوافق مع بروتوكولات شبكات **Netware** أو **Windows**.
- هذا البروتوكول سهل الإعداد فعندما ترغب في إضافته، كل ما عليك هو النقر فوق

بعض الأزرار في Network Control Panel.

طبقات نموذج TCP/IP

يشتمل TCP/IP علي أربعة طبقات . وهذه الطبقات هي :

١– طبقة التطبيق Application Layer

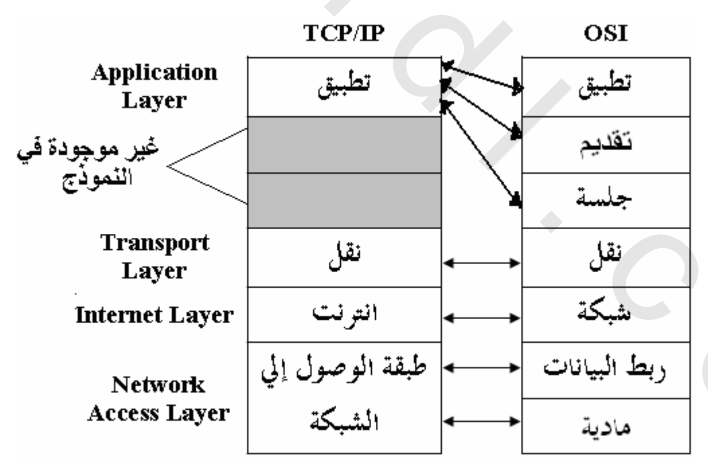
٢– طبقة النقل Transport Layer

٣– طبقة الانترنت Internet Layer

٤– طبقة الوصل إلي البيانات Network Access Layer

وكما تلاحظ بعض هذه الطبقات تأخذ أسماء طبقات نموذج OSI. ورغم هذا التشابه في تسمية الطبقات إلا أن وظيفة الطبقة تختلف من نموذج لآخر حتي وإن تسمت بنفس الاسم. لأن هذه الطبقات الأربعة من المفروض أن تؤدي الوظائف التي تؤديها الطبقات السبع الموجودة في نموذج OSI

يشتمل شكل ٧–١ علي طبقات TCP/IP الأربعة ومكافئ كل منها مع نظيرها في نموذج OSI .



شكل ٧–١ الطبقات المكافئة لنموذج TCP/IP في نموذج OSI

طبقة التطبيق The Application Layer

لا يملك نموذج TCP/IP طبقتي الجلسة والتقديم وذلك لأنه لم تظهر الحاجة لهما. وقد أثبتت التجربة مع نموذج OSI صحة هذه المقولة فهما قلما تستخدمان لمعظم التطبيقات.

تقع طبقة التطبيق فوق طبقة النقل.

بروتوكولات طبقة التطبيق

تدعم البروتوكولات العاملة علي طبقة التطبيق نقل الملفات والبريد الالكتروني والاتصال عن بعد ..... الخ . نوضح فيما يلي أهم البروتوكولات العاملة علي هذه الطبقة. (انظر شكل ٧-٢)

- *بروتوكول نقل الملفات* **File Transfer Protocol (FTP)**

يعتبر بروتوكول FTP من أشهر البروتوكولات المستخدمة لنقل الملفات بين الأنظمة التي تدعم FTP . وهو يدعم نقل الملفات التي تأخذ الشكل الثنائي (Binary) والملفات التي تستخدم شفرة ASCII .

- *بروتوكولات نقل البريد البسيط* **Simple Mail Transfer Protocol (SMTP)**

بروتوكول SMTP هو المسئول عن نقل رسائل البريد الالكتروني عبر شبكة الاتصالات . وهو بذلك لا ينقل إلا البيانات النصية التي تحتوي عليها الرسائل .

- *بروتوكول مكتب البريد* **Post Office Protocol (POP3)**

يستخدم عملاء البريد الالكتروني بروتوكول POP3 للحصول علي رسائلهم من وحدة خدمة البريد الالكتروني

- *نظام أسماء النطاقات* **Domain Name System (DNS)**

هو نظام موجود علي الانترنت لترجمة أسماء النطاقات إلي عناوين IP (IP Addresses) . عندما تتصل بموقع موجود علي الانترنت ، يقوم DNS بتحويل اسم الموقع إلي عنوان IP الذي يحتاجه بروتوكول TCP/IP للاتصال بالجهاز المضيف للموقع .

- *بروتوكول الإدارة البسيط للشبكات* **Simple Network Management Protocol (SNMP)**

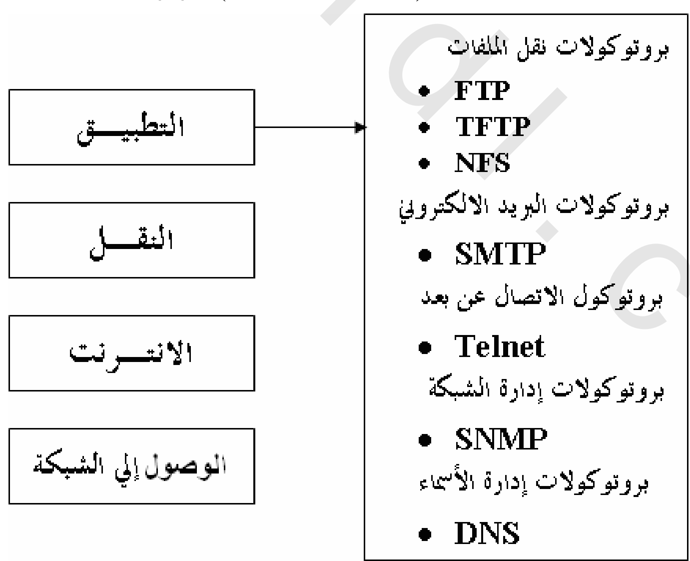
يقدم بروتوكول **SNMP** طريقة للتحكم في إدارة مكونات الشبكة . بروتوكول **SNMP** مسئول أيضاً عن جمع معلومات عن مكونات الشبكة وعن تحسين أدائها وتأمينها .

نظام ملفات الشبكة **Network File System (NFS)**

يسمح بروتوكول **NFS** بالوصول إلي الملفات الموجودة علي وحدات تخزين بعيدة كالأقراص المغناطيسية عبر شبكة الاتصال .

بروتوكول **Telnet**

Telnet هو بروتوكول يسمح بالاتصال عن بعد بالأجهزة الموجودة علي الشبكة والتحكم فيها . يستخدم **Telnet** للتحكم عن بُعد بكمبيوتر في موقع آخر بعد الاتصال به وتنفيذ أي عملية عليه وفي هذه الحالة فإن الكمبيوتر البعيد هو الذي ينفذ العملية وليس الجهاز المحلي. يقال عن الجهاز المحلي "مضيف محلي" (**Local Host**) ويقال عن الجهاز البعيد الذي ينفذ العملية " المضيف البعيد " (**Remote Host**) أو وحدة خدمة **Telnet**.



شكل ٧–٢ بروتوكولات طبقة التطبيق

طبقة النقل The Transport Layer

تدعى الطبقة التي تعلو طبقة انترنت فى نموذج **TCP/IP** بطبقة النقل، وهى مصممة لكي تسمح لزوج من العناصر فى المرسل والمستقبل أن يقيما محادثة فيما بينهما تماما كما فى طبقة النقل من نموذج **OSI**.

بروتوكولات طبقة النقل

لقد تم تعريف بروتوكولين من نوع طرف إلى طرف **end-to-end** فى هذه الطبقة وهما بروتوكول **TCP** وبروتوكول **UDP** (أنظر شكل ٧-٣)

أولاً: بروتوكول التحكم بالنقل TCP(Transmission Control Protocol)

وهو بروتوكول اتصال موثوق موجه وهو يسمح لسلسلة من البيانات مولدة فى جهاز مصدر أن تصل بشكل صحيح إلى الهدف. يقوم بروتوكول **TCP** بالمهام الآتية :

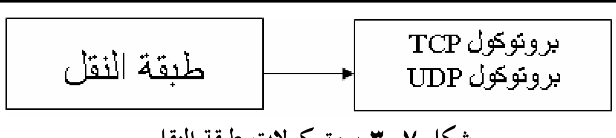
- *تجزئة وتجميع البيانات* :ويقوم بروتوكول **TCP** بتجزئة البيانات الواردة إلى رزم صغيرة يقوم بتمريرها إلى طبقة انترنت فى الجهاز الهدف (المستقبل) ، ويقوم إجراء **TCP** فى الجهاز المستقبل بإعادة تجميع هذه القطع وإعادها إلى شكل السلسلة المرسلة الأصلية ، لأن قيام أي جهاز بإرسال بياناته بصفة مستمرة لمدة من الزمن يسبب بطء الشبكة "زحمة المواصلات" مما يؤدي إلي انتظار الأجهزة الأخرى الموجودة علي نفس الشبكة لمدة طويلة من الزمن ، حتي ينتهي الجهاز المرسل من تحويل كل بياناته . عملية تجزئة البيانات تسمح للأجهزة الموجودة علي الشبكة بالتناوب في استخدام الشبكة . وفي حالة حدوث خطأ لا يعيد الجهاز المرسل إلا الجزء الخطأ فقط بدلاً من إعادة إرسال كل البيانات من جديد .
- *الإشعار بالاستلام* : عندما يستقبل جهاز رزمة بيانات بدون خطأ ، فإنه يرسل للجهاز المرسل إشعار يفيد استقبال واستلام البيانات حتى يستطيع الجهاز المرسل متابعة إرسال الرزمة التالية
- *تحديد المنافذ* (**Ports**) : تحدد بروتوكولات طبقة النقل أرقام المنافذ التي تمر منها

البيانات إلي مناطق معينة في ذاكرة الجهاز والتي غالباً ما تخص تطبيق معين . وبهذا يستطيع بروتوكول TCP تمييز العملية التي ولدت البيانات الواردة من طبقة التطبيق

- *الكشف عن الأخطاء :* طبقة النقل هي المسئولة عن كشف الأخطاء التي تحدث لرزم البيانات أثناء النقل . في حالة الإرسال ، يدقق النظام في إطار البيانات المرسل ويقوم بعملية حسابية علي إطار البيانات ، ويضع النتيجة التي يحصل عليها في تذييل الإطار (Frame Trailer) وعندما تصل البيانات إلي المستقبل ، يقوم الجهاز المستقبل بإجراء نفس العملية الحسابية علي البيانات التي يستقبلها . إذا كانت النتيجة مطابقة للنتيجة المرفقة في تذييل الإطار ، فهذا معناه أن البيانات سليمة وتتم معالجة البيانات . أما إذا لم تتطابق النتائج ، فإن النظام يطلب إعادة إرسال البيانات مرة ثانية.
- *التحكم في تدفق البيانات :* يقوم TCP بالتحكم بتدفق البيانات لمنع المرسل السريع من إغراق المستقبل البطيء بالبيانات.
- *ترقيم رزم البيانات :*من مهام طبقة النقل ترقيم رزم البيانات عند إرسالها وترتيبها عند الاستلام ، وذلك لأن الرزم تسلك مسارات مختلفة في رحلتها من الجهاز المرسل إلي الجهاز المستقبل لأنها تختار المسارات الأقل زحمة . وهذا يسبب وصول الرزمة إلي وجهتها بترتيب غير الترتيب الذي أرسلت به. لولا ترقيم الرزم في الإرسال لما تمكن النظام من ترتيبها عند الاستقبال .

ثانياً: بروتوكول مخطط بيانات المستخدم **User Datagram Protocol (UDP)**.

وهو بروتوكول لاتصال غير موثوق ومناسب للتطبيقات التى يكون فيها الإعلام بالاستلام أهم من حصوله فعلا مثل حالات نقل الكلام أو الفيديو. عندما نقوم بإرسال بواسطة UDP فليس هناك ضمان أن البيانات تصل إلي وجهتها بدون خطأ . وهو مستخدم أيضاً من أجل الاستعلامات من نمط وحدة خدمة / محطة عمل والتي تطلب لمرة واحدة فقط .



شكل ٧-٣ بروتوكولات طبقة النقل

طبقة الانترنت The Internet Layer

من مهام طبقة الانترنت توجيه الرزم إلي الأجهزة التي يطلب توجيهها إليها ، سواء كانت هذه الأجهزة موجودة علي شبكة محلية أو علي شبكة واسعة . وبالتالي يتضح لنا أن عملية توجيه الرزم هو أهم عمل تقوم به هذه الطبقة بالإضافة إلى تعديل الرزم **Packet Switching** ، ولهذا السبب فإنه يمكن أن نقول أن طبقة انترنت فى بنية **TCP/IP** تقابل طبقة الشبكة فى بنية **OSI** .

يمكن لهذه الرزم أن تصل بترتيب مختلف عن الترتيب الذي أرسلت به، ويكون دور الطبقات الأعلى هو إعادة تجميع وترتيب هذه الرزم إذا كان الترتيب مطلوبا فى جهة المستقبل.

إضافة إلي ذلك تكون هذه الطبقة مسئولة عن توفير المعلومات اللازمة إلي طبقة الوصول إلي الشبكة لكي تتمكن هذه الأخيرة من إرسال إطاراها علي الشبكة المحلية سواء كان الهدف جهازاً أو موجه .

ويمكن تشبيه عمل هذه الطبقة بنظام البريد، حيث يقوم المستخدم بوضع عدد من الرسائل بشكل متتالي فى صندوق البريد فى أحد البلدان، وبقليل من الحظ سوف يتم تسليم هذه الرسائل إلى وجهتها فى البلدان الأخرى، وقد تعبر هذه الرسائل عددا من مكاتب البريد العالمية فى طريقها إلى هدفها، ولكن ذلك يبقى غير مرئي من قبل المرسل، وأكثر من ذلك فقد يكون لكل بلد من البلدان الذي ستعبر خلاله الرسائل نظام بريد خاص به، وطوابع خاصة به، ومواصفات مغلفات رسائل معينة وكل ذلك من الأمور التى لن يتعامل معها المرسل أو يعالجها.

فيما يلي نوضح باختصار البروتوكولات التي تعمل في طبقة الانترنت (انظر شكل ٧-٤)

- ***بروتوكول الانترنت*** **Internet Protocol (IP)**

يعتبر IP أهم بروتوكول في هذه الطبقة ، لا يهتم IP بمحتويات الرزمة ولكنه يهتم بطريقة توجيه الرزم إلي الوجهة (سواء كانت جهاز أو موجه) ويقوم بمهمة العنونة والإرسال .

- ***بروتوكول التحكم في رسائل الانترنت*** **Internet Control Message Protocol (ICMP)**

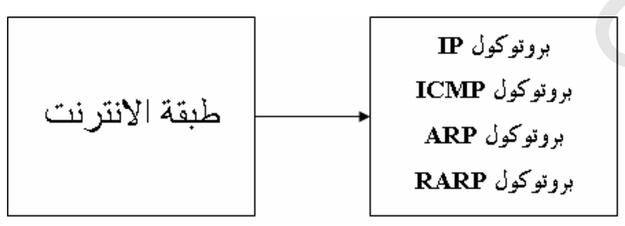
يوفر ICMP إمكانيات التحكم في الرسائل وإرسالها ، بالإضافة إلي إمكانية تبادل معلومات حول مشاكل وأعطال الشبكة إذا حدثت .

- ***بروتوكول حل العناوين*** **Address Resolution Protocol (ARP)**

يقوم بتحويل عنوان IP لجهاز موجود علي الشبكة المحلية إلي عنوان MAC (الحروف MAC اختصاراً لعبارة Media Access Control ومعناها "التحكم في وصول الوسائط") وهو عنوان فريد لكل بطاقة شبكة ويبلغ طوله ٦ بايت (48 bits) . ويتم تمثيله باستخدام الرموز السداسية العشرية (Hexadecimal) . يمكن أن يكون هذا العنوان هو عنوان الوجهة إذا كان الجهازين علي نفس الشبكة المحلية أو عنوان الموجه إذا كان الجهازان علي شبكتين مختلفتين .

- **Reverse Address Resolution Protocol (RARP)**

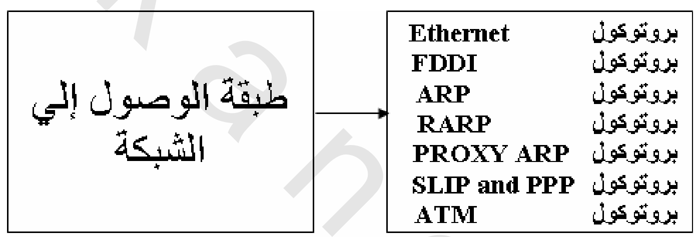
يقوم RARP بتحويل أي عنوان MAC إلي عنوان IP وهو يستخدم عنوان MAC للجهاز لإعطاء الجهاز عنوان IP وإمكانية توصيله بالشبكة



شكل ٧–٤ بروتوكولات طبقة الانترنت

طبقة الوصول إلى الشبكة Network Access Layer

تسمى هذه الطبقة أيضا **The Host-to-Network Layer** ومعناها "طبقة المضيف – الشبكة" . أى جهاز مضيف يريد أن يصل إلى الشبكة باستعمال بروتوكول ما، فأنه يستطيع أن يرسل رزم **IP** عبر هذه الطبقة. تكافئ هذه الطبقة كل من طبقتي "ربط البيانات" و "المادية" في نموذج **OSI** ومن مهامها أيضا تحويل البتات إلي إشارات كهربية أو كهرومغناطيسية أو ضوئية ليمكن نقلها علي الوسيط المعني بالأمر . تحول بروتوكولات طبقة الوصول إلي البيانات عناوين **IP** إلي عناوين مادية للأجهزة وتضع رزم **IP** داخل أطر (انظر شكل ٧–٥) . أيضا تحدد الوسيط المادي اللازم للاتصال بناء علي نوع الجهاز وبطاقة الشبكة .



شكل ٧–٥ بروتوكولات طبقة الوصول إلي الشبكة

عناوين IP

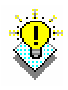
نشرح فيما يلي باختصار عناوين **IP** علي أن نعود لشرح فئات العناوين وكيفية تخصيصها بالتفصيل في الفصل السابع عشر .

يستخدم بروتوكول **TCP/IP**عناوين مخصوصة تعرف باسم عناوين**IP** . لتعريف أجهزة الكمبيوتر المختلفة المتصلة بالانترنت. ولكن ماهو عنوان **IP**. عنوان **IP** عبارة عن رقم مكون من ٣٢ بت يتكون عادة من ٤ أرقام عشرية متتابعة تنفصل عن بعضها البعض بنقاط لان كل رقم عشري يتكون من ٨ بت (٤X٨=٣٢).

انظر عنوان **IP** العشري المنقط التالي **192 . 168 . 100 . 25**

ونظرا لأن هناك أربعة أرقام يبلغ طول كل منها(**8 Bits**)فإن مساحة العنوان الإجمالية يبلغ طولها٣٢بت (**32 Bits**) وبالتالي يبدو العنوان السابق عند كتابة بالنظام الثنائي (**Bits**)

هكذا: **11000000.10101000.01100100.00011001**



للمزيد من المعلومات عن النظام الثنائي والنظام العشري والنظام السداسي عشر، راجع تمثيل البيانات داخل ذاكرة الكمبيوتر في الفصل الثالث.

ومن التمثيل السابق تلاحظ أن العنوان الثنائي يشتمل علي ٤ مجموعات يفصل بين كل منها نقطة، كل مجموعة بها ٨ بتات، وبذلك يكون العنوان ٣٢ بت (البت أما صفر أو واحد).

تخصص لشبكتك الأرقام الثلاثة أو الأربعة الأولي من العنوان (تبعا لحجمها) بينما يُعَرفَّ بقية العنوان جهاز الكمبيوتر المتصل بالشبكة .

وفي حالة اتصال شبكتك بالانترنت، فلن يتمكن أي جهاز علي الشبكة من الوصول إليها إلا من خلال عنوان IP الخاص به. لا يتم تخصيص هذه العناوين للأجهزة يدويا .

ولكن تقوم وحدة خدمة خاصة (تعرف باسم وحدة خدمة DHCP) بتخصيص هذه العناوين تلقائيا .

في حالة الاتصال بالانترنت من خلال مزود خدمة اتصال (ISP) ، يمكنك الاعتماد علي وحدة خدمة DHCP الخاصة به في تخصيص عناوين IP إن وجدت، فإن لم توجد يمكن تهيئة وحدة خدمة Windows أو Network للعمل كوحدة خدمة DHCP للشبكة .

ما سبب أهمية العناوين

مثلما يحصل للعناوين البريدية حيث يخصص لكل شخص عنوان بريدي فريد يحدث أيضا مع الانترنت، حيث تتطلب الانترنت أسماء وعناوين فريدة. تتوفر مساحة قدرها ٣٢بت لعناوين الانترنت. مساحة ٣٢بت تتسع لمعالجة أربعة ملايين عنوان. وبمجرد إن يتم استخدام مساحة العناوين التي تبلغ أكثر من٤ ملايين، لن يكون هناك مساحة لكتابة أية عناوين إضافية. لذلك يعد الجيل التالي من بروتوكول الانترنت (Protocol Internet) الذي يطلق عليه IPV6 مهم جدا لأنه يزيد عدد العناوين لعدد كبير جدا.

فئات العناوين

تأتى كتل العناوين فى ثلاثة إحجام اعتمادا على فئة العنوان على النحو التالي :

- **عناوين الفئة A : يمكن أن تحدد الفئة A عدد عناوين يصل إلى ١٦,٧٧٧,٢١٦ عنوان فى كل شبكة اتصال من ١٢٦ شبكة اتصال.**
- **عناوين الفئة B : يمكن أن تحدد الفئة B عدد عناوين يصل إلى ٦٥,٥٣٦ عنوان فى كل شبكة اتصال من ١٦,٣٨٢ شبكة اتصال.**
- **عناوين الفئة C : يمكن أن تحدد الفئة Cعدد عناوين يصل إلى ٢٥٦ عنوان فى كل شبكة اتصال من ٢,٠٩٧,١٥٠ شبكة اتصال.**

ومن هذا التوضيح لطريقة عنونة IP، يتضح أن هذا النظام فى تخصيص العناوين يعتبر مصدرا للعناوين. حيث أنه فى ظل عناوين الانترنت التى تبلغ ٣٢بت الحالى، يجب أن تحدد المؤسسات فئة الشبكة التى سوف توفر عناوين IP كافية لاحتياجاها.

ونضرب مثالاً واحداً. بالنسبة لعناوين الفئة C والتى تخص الشبكات الصغيرة. المؤسسة التى تطلب عنوان كاملا من الفئة C، سوف يخصص لها ٢٥٦ عنوان، حتى أذا طلبت ٢٠ عنوانا فقط. وبالمثل تستطيع أن تفهم أن المؤسسات التى تطلب أكثر من ٢٥٦ عنوان وهى المؤسسة التى تقع فى الفئة Bسوف يخصص لها ٦٥٢٣٦ عنوان حتى ولو كانت لا تحتاج إلا إلى ٣٠٠ عنوان.

عناوين IPV6

IPV6 هى الجيل التالى من بروتوكول IP.حيث أن الجيل الحالى من IP هو IPV6. يحل IPV6 مشكلة العناوين لأن الأربعة ملايين عنوان إذا كنت تراها كثيرة، فهى مع الانتشار السريع للانترنت لن تكون كافية لتلبية طلبات الجهات التى تطلب عناوين انترنت.

تستخدم IPV6 مساحة عناوين تبلغ ١٢٨بت مقابل المساحة المتوفرة فى بروتوكولIPV4 وقدرها ٣٢بت. أيضا يتم تخطيط بروتوكول IPV6 بطريقة مختلفة عن IPV4 حيث تمثل كل Xستة عشر بت مكتوبة برموز سداسية عشرية (من 0الىF)

فيما يلى مقارنة بين عنوان IPV4 وعنوان IPV6.

أولاً IPV4:

X.X.X.X حيث تمثل كل X٨بتات فى الرموز العشرية المنقطة وعندما تضرب ٤X٨ تحصل على ٣٢ وهو طول المساحة المخصصة لبروتوكول IPV4.

ثانياً IPV6:

X:X:X:X:X:X:X:X حيث تمثل كل X ستة عشر بت مكتوبة برموز سداسيه عشرية وعندما تضرب ٨X١٦ تحصل على ١٢٨وهو طول المسافة المخصصة لبروتوكول IPV6.

مقارنة بين النموذج OSI والنموذج TCP

يشترك النموذجان فى عدة نقاط، فكلاهما مبنى على فكرة تكديس بروتوكولات مستقلة عن بعضها، فوق بعضها، كما أن هناك تشابها لا بأس به فى وظيفة كل طبقة، فمثلا جميع الطبقات التى فوق طبقة النقل بما فيها طبقة النقل لها وظيفة عامة هى تزويد الإجراءات التى تريد التواصل بخدمة نقل مستقلة عن الشبكة ومن نمط نقطة إلى نقطة.

ومن جهة أخرى، هناك العديد من الفروقات بينهما،

فيما يلي نوضح باختصار أولاً أوجه الشبه بين النموذجين ثم نوضح باختصار أيضا أوجه الاختلاف بينهما .

أوجه الشبه

- كل من النموذجين يحتوي علي طبقات
- كل من النموذجين يحتوي علي طبقة التطبيق رغم أن كل منهما تقدم خدمات مختلفة
- كلا النموذجين يحتوي علي طبقتي النقل والشبكة
- كلا النموذجين يستخدم تقنية تبديل الرزم (Packet Switching) بدلاً من تقنية تبديل الدوائر (Circuit Switching)

أوجه الاختلاف

- في نموذج TCP/IP يتم دمج طبقات التطبيق والتقديم والجلسة في طبقة واحدة

هي طبقة التطبيق

- في نموذج TCP/IP يتم دمج طبقتي ربط البيانات والمادية في طبقة الوصول إلي الشبكة
- يبدو نموذج TCP/IP بسيطاً لأنه يحتوي علي أربع طبقات بدلاً من سبعة
- عندما تستخدم طبقة النقل في نموذج TCP/IP بروتوكول UDP فأنها لا تقدم أي ضمان لوثوقية رزم البيانات بينما تتحقق طبقة النقل في نموذج OSI من صحة ودقة البيانات المرسلة .

عيوب النموذج المرجعي TCP/IP

إن النموذج TCP/IP وبروتوكولاته لها بعض المشاكل.

أولا : لا يميز النموذج بوضوح بين مفاهيم الخدمة والواجهة والبروتوكول، ومن صفات التصميم الهندسي الجيد لأي عتاد لين هو التمييز بين التوصيف وتحقيق هذا التوصيف على أرض الواقع.

ثانيا: إن TCP/IP ليس نموذجا عاما وهو لا يتوافق بشكل جيد مع مكدسات بروتوكولات أخرى غير بروتوكول TCP/IP .

ثالثا: إن طبقة Network Access ليست طبقة حقيقية بالمعنى المستخدم فى توصيف البروتوكولات المبنية على الطبقات، ولكنها عبارة عن واجهة وصل بين طبقة الشبكة وطبقة ربط البيانات، وموضوع التمييز بين الطبقة والواجهة مهم جدا ويجب أن يكون دائما واضحاً في الأذهان .

رابعا: لم يميز نموذج TCP/IP بين الطبقة المادية وطبقة ربط البيانات، وحتى أنه لم يذكرهم بوضوح بالرغم من إنهما مختلفتين كليا.

ملخص الفصل

بدأنا في هذا الفصل بشرح المقصود ببروتوكول TCP/IP ثم شرحنا طبقات نموذج TCP/IP . شرحنا أيضا الفرق بين نموذج OSI ونموذج TCP/IP. شرحنا بعد ذلك

عيوب النموذج .TCP/IP

تدريبات

١. أنشأت هيئة IETF بروتوكول TCP/IP من أجل:

أ. أن يكون مقياسا مفتوحا لا تتحكم فيه أي شركة

ب. أن يعمل على نقل البيانات من وإلى أجهزة الكمبيوتر عبر شبكة الانترنت

ج. أن يستخدم أي نوع من الكابلات

د. أن يتوافق مع بروتوكولات شبكات Netware أو Windows

هـ. كل ما سبق

و. لا شئ مما سبق

٢. أي العبارات التالية صح عند مقارنة نموذج TCP/IP بنموذج OSI

أ. يستخدم نموذج TCP/IP الطبقات الأربعة الأولى من نموذج OSI

ب. يشتمل نموذج TCP/IP على أربعة طبقات فقط في مقابل ٧ طبقات في نموذج OSI

ج. كلا النموذجين يستخدم طبقتي النقل والشبكة

د. تقابل كل من طبقة التطبيق والتقديم والجلسة طبقة نظيرة في كلا النموذجين

هـ. تقابل طبقة الوصول إلى الشبكة في نموذج TCP/IP الطبقة المادية في نموذج OSI

٣. ما هي الطبقة التي يعمل عليها أي من البروتوكولات التالية في نموذج TCP/IP :

أ. SMPT   د. FTP

ب. ARP   هـ. IP

ج. TCP   و. UDP

٤. البروتوكول الذي يولد إشعار باستلام البيانات هو:

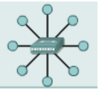
أ. UDP   ج.TCP

ب. IP   د. ARP

٥. صل الإجابة الصحيحة والتي تحدد المصطلحات والوظائف التي تخص كل طبقة من

طبقات TCP/IP

أ. **تدعم البروتوكولات العاملة على هذه الطبقة نقل البيانات (FTP) والبريد الالكتروني (SMTP) والاتصال عن بعد (Telnet)....الخ**	١. **الانترنت**
ب. **تقابل هذه الطبقة طبقة الشبكة في نموذج OSI وتقوم بتوجيه الرزم إلى الأجهزة التي يطلب توجيهها إليها وتقوم أيضا بتعديل الرزم (Packet Switching). تستخدم بروتوكولات مثل ARP, ICMP, IP**	٢. **التطبيق**
ج. **تكافئ هذه الطبقة طبقتي ربط البيانات والمادية في نموذج OSI. تحول عناوين IP إلى عناوين مادية للأجهزة**	٣. **النقل**
د. **هي الطبقة التي تعلو طبقة الانترنت وهي مصممة لكي تسمح لزوج من العناصر في المرسل والمستقبل ثم يقيما محادثة فيما بينهما وتستخدم بروتوكولي UDP, TCP.**	٤. **الوصول إلى الشبكة**



الباب الثالث
مكونات الشبكة

الفصل الثامن : أجهزة ذووسائط الاتصال

الفصل التاسع : وحدة الخدمة (Server)

الفصل العاشر : نظم تشغيل الشبكة



نستكمل في هذا الفصل شرح أجهزة ووسائط الاتصال ونركز في هذا الفصل علي موضوعين رئيسين الأول أجهزة الشبكة والثاني أنواع الكابلات ومواصفاتها .

بالانتهاء من هذا الفصل ستتعرف علي :

- ***أجهزة توصيل الشبكة***
- ***بطاقة الشبكة (NIC)***
- ***أنواع الكابلات ومواصفاتها***

أجهزة التوصيل

إذا كان لديك أكثر من جهازى كمبيوتر وتستخدم شبكة محلية من نوع نظير لنظير (Peer-to-Peer) وتستخدم تخطيط الناقل (Bus Topology) فلن تحتاج إلى أحد أجهزة التوصيل . إما إذا كان لديك أكثر من جهازى كمبيوتر فى شبكة اتصال كبيرة تستخدم بنية نجمية أو حلقية فستحتاج إلى جهاز لتوصيل أجهزة الكمبيوتر الإضافيه به. وتشمل أجهزة التوصيل مايلى:

- وحدة توصيل (hub) ويعتبر أبسط أجهزة التوصيل.
- مبدل (Switch)
- جسر (Bridge)
- موجه (Router)

وحدات التوصيل (hub)

وحدة التوصيل عبارة عن صندوق يتصل به كل شئ وتسمي أيضا وحدة التجميع والاسم الانجليزي لها هوHUB . في الشبكات التي تستخدم وحدات توصيل لم تعد تمر الأسلاك التي تصل أجهزة الكمبيوتر من جهاز لآخر. ولكنها تمر من وحدة توصيل إلي محطة العمل (Work Station) في توصيف نجمي .

تستخدم وحدات التوصيل ليس فقط لتوصيل محطات العمل بوحدة الخدمة ولكن أيضا لتوصيل أى أجهزة أخرى على الشبكة مثل وحدات خدمة أخرى أو طابعات أو وحدات توصيل أخرى . تحتوي وحدات التوصيل الصغيرة علي ٤ منافذ ، أما وحدة التوصيل الكبيرة فتحتوي علي أكثر من ٢٤ منفذ (انظر شكل ٨-١)



شكل ٨-١ صورة لإحدى وحدات التوصيل

تعمل وحدات التوصيل عند الطبقة السفلى من نموذج OSI وهى الطبقة المادية (Physical) مع تكرار المعلومات التى تتلقاها. تلتقط وحدة التوصيل الإشارة من أحد الأسلاك ، ثم تضخمها وترسلها إلي باقي الأسلاك . بمعني أن وحدة التوصيل عندما تستلم الإشارة الكهربية الموجودة علي الكابل تقوم بتكبيرها وإرسالها إلي جميع المنافذ الأخرى دون أن تعلم إلي أي جهاز و أين ستتجه هذه الإشارات .

لا تقوم وحدة التوصيل بتصفية المعلومات التى ترد إليها ، ولا توجهها إلى وجهتها الصحيحة لأنها تأخذ كل ما يرد إليها فى خط واحد وتضعه على كل الخطوط الأخرى. معنى ذلك أن أى محطة موجودة على الشبكة يمكنها أن تسمع ما تضعه أى محطة أخرى على الشبكة. مع زيادة تدفق الاتصالات، يزداد عدد التصادمات بين الإطارات. مما يتسبب فى حدوث مشكلة تسمى Device Contention أو (التنازع على الأجهزة).

ربط وحدات التوصيل

قلنا أن وحدات التوصيل تحتوى على عدد من المنافذ من ٤ إلى ٢٤ يعنى يمكن توصيل عدد من الأجهزة يصل إلى ٢٤ جهاز باستخدام وحدة التوصيل. لكن ما العمل إذا أردنا زيادة الشبكة نتيجة للتوسعات التى طرأت على المؤسسة. يمكننا توصيل وحدة توصيل ثانية لنتمكن من زيادة عدد الأجهزة الموصلة بالشبكة

تحتوى وحدات التوصيل على منفذ إضافى يسمى منفذ الربط التوسعى Uplink Port. يستخدم هذا المنفذ خصيصا للربط مع وحدة توصيل أخرى وليس بجهاز كمبيوتر آخر.

ولذلك فإن طريقة توصيل هذا المنفذ تختلف عن طريقة توصيل المنافذ الأخرى.
لا يحتوى منفذ الربط التوسعى على دوائر العبور **Crossover Circuit** الموجــودة فى المنافذ العادية والتى تتلخص مهمتها فى توصيل أسلاك الإرسال فى كابل **UTP** من جهاز ما إلى أسلاك الاستقبال للأجهزة الأخرى.
تحقق خاصية عدم وجود دوائر العبور فى منفذ الربط التوسعى إمكانية ربط المنفذ التوسعى لوحدة التوصيل الأولى بمنفذ عادى من وحدة التوصيل الثانية. وبهذا تــتمكن الأجهــزة المربوطة مع وحدة التوصيل الأولى من الاتصال مع الأجهزة المربوطة مع وحدة التوصـــيل الثانية لأننا سنستخدم فى هذه الحالة دوائر عبور وحدة التوصيل الثانية.
أما إذا ربطنا المنفذ التوسعى لوحدة التوصيل الأولى مع المنفذ التوسعى لوحدة التوصـــيل الثانية، فستتصل أسلاك إرسال الأجهزة المربوطة بالوحدة الأولى بأسلاك إرسال الأجهــزة المربوطة بالوحدة الثانية، مما يؤدى إلى عدم اتصال الأجهزة مع بعضها. لأن منفذى الربط التوسعى لوحدة التوصيل لا يحتويان على دوائر عبور.

المبدلات (Switches)

يحتوى المبدل– مثل وحدة التوصيل –على عدد من المنافذ يتراوح بــين ٤و٢٤ انظر شكل ٨–٢



شكل ٨–٢ صورة لأحد المبدلات

على العكس من وحدة التوصيل التى لا تقوم بتصفية أو معالجة البيانات التى تتدفق خلالها، يعد المبدل جهازا ذكيا. حيث يقوم بإلقاء نظرة على عنوان الوجهة الخاص بالإطار المتدفق فيه ويقوم بتوجيه الرزمة فقط إلى المنفذ الموصل بجهاز الوجهة أو المستقبل (علــى عكــس وحدة التوصيل التى توجه كل الرزم الواردة إلى كل المنافذ) . ولتوضيح الفرق بين أجهزة وحدة التوصيل **HUB** وأجهزة المبدلات **Switch** نقول: تتسم أجهزة المبدلات بفاعليــة

أكبر من أجهزة وحدات التوصيل **HUB** ترجع إلي سرعتها وإلي عوامل أخري تتضح مما يلي :

يعمل جهاز الـــ **HUB** علي توجيه أية حزمة بيانات تصل إليه علي أي منفذ من منافذه تلقائيا إلي جميع المنافذ الأخرى. والسبب أن جهاز وحدة التوصيل **HUB** لا يعلم المنفذ المتصل به كل جهاز كمبيوتر. لنفرض أن جهاز فريد متصل بمنفذ١ في جهاز وحدة توصيل (**HUB**) مكون من ثمانية منافذ وأن جهاز وليد متصل بمنفذ ٥، إذا أرسل جهاز وليد حزمة بيانات إلي جهاز فريد فإن وحدة التوصيل **HUB** تستقبل الحزمة علي منفذ ١ ثم ترسلها إلي جميع منافذه الأخرى من ٢ إلي ٨ وبذلك تري جميع الأجهزة الأخرى المتصلة بوحدة التوصيل **HUB** حزمة البيانات وتقرر ما إذا كانت موجهة لها أم لا .

علي العكس عند الاستخدام جهاز المبدل **Switch** ، إذا أرسل جهاز فريد المتصل بمنفذ ١ حزمة بيانات إلي جهاز وليد علي منفذ ٥، فإن جهاز المبدل **Switch** يستقبل حزمة البيانات علي منذ ١ ثم يرسلها إلي منفذ٥ فقط. بذلك يتحقق قدر أكبر من السرعة ومن التأمين لأن جهاز الكمبيوتر لن يري إلا حزم البيانات الموجهة إليه فقط .

عندما يرسل جهاز بيانات إلى جهاز آخر داخل الشبكة يقرأ المبدل البيانات الموجودة فى ترويسة الإطار وبالضبط العنوان المادى للجهاز المستقبل ثم يخصص قناة مادية بين الجهازين. ويحدث نفس الشئ عندما يرغب جهاز فى الاتصال بجهاز آخر فى نفس الوقت. معنى هذا أن كل رزمة تأخذ مسارا مخصصا لها من الجهاز المصدر إلى الجهاز الوجهة. وهكذا يستطيع كل جهاز أن يكون لديه قناة خاصة تربطه بالجهاز الذي يرغب فى التخاطب معه وهذا معناه أن الشبكة تكون خالية من التصادم والازدحام وبالتالى لن تحدث مشكلة **Device Contention** "التنازع على الأجهزة" التى تحدث مع وحدات التوصيل.

بالإضافة إلى ميزة منع التصادمات والزحام، يوفر المبدل ميزة أخرى تزيد من أداء الشبكة. تلك هى تخصيص كامل عرض النطاق (**Bandwidth**) لكل زوج من الأجهزة المتصلة مع بعضها.

تقوم المبدلات (مثل الجسور والموجهات) بتقسيم شبكة الاتصال إلى مقاطع لتقليل تدفق

البيانات وبالتالى التنازع على الأجهزة. يمكن تقسيم مقاطع المبدلات عند أى مستوى يمكن أن يكون لديك عنده وحدة التوصيل أو جسر أو موجه. يعمل المبدل عند طبقة ربط البيانات فى نموذج OSI.

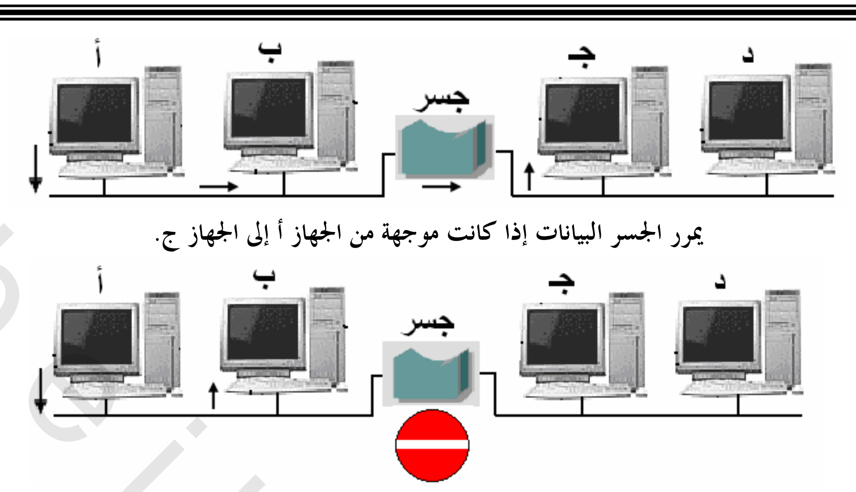
الجسور **Bridges**

تستخدم الجسور أساسا لربط شبكتى اتصال معاً، أو لتقسيم شبكة اتصال إلى مقاطع. الهدف من استخدام الجسر هو تقليل تدفق الاتصالات فى الشبكة عن طريق تقسيم الشبكة رغم أنها ستبقى شبكة واحدة. عندما تقوم بربط شبكتى اتصال باستخدام الجسر، تحصل على شبكة اتصال واحدة بمقطعين.

إذا أراد جهازان موجودان على المقطع الأول من الشبكة الاتصال ببعضهما، فإن نطاق تبادل الرسائل والبيانات سيبقى متعلقا بالمقطع الأول من الشبكة المجزئة، ولن يتأثر المقطع الثانى من الشبكة. هذا الأمر يؤدى إلى نقص فى التصادمات وبالتالى تحسين أداء الشبكة كلها.

أما فى حالة رغبة جهاز موجود على المقطع الأول من الشبكة الاتصال بجهاز موجود على المقطع الثانى من الشبكة، فإن البيانات فى هذه الحالة فقط يمكنها العبور من المقطع الأول إلى المقطع الثانى. يقرأ المبدل العنوان المادى للجهاز المستقبل ويبنى قراره بالإبقاء على رزم البيانات أو توجيهها بناء على موقع الجهاز من الشبكة المجزأة. فإذا كان موقع الجهاز المستقبل (الجهاز الوجهة) على المقطع الثانى من الشبكة والجهاز المرسل على المقطع الأول يقرر المبدل تحرير رزمة البيانات إلى المنفذ الثانى ، أما إذا كان عنوان الجهاز المستقبل (الجهاز الوجهة) موجود فى نفس مقطع الجهاز المرسل، فإن المبدل يتجاهل هذه الرزمة. وهذا ما يتضح من خلال شكل ٨-٣

يتسبب تقليل حركة النقل فى زيادة سرعة الشبكة. لأن الجسر ينظر إلي العنوان المادى لجهاز الوجهة، يعمل الجسر على مستوى طبقة ربط البيانات فى نموذج OSI المرجعى.



يمرر الجسر البيانات إذا كانت موجهة من الجهاز أ إلى الجهاز ج.

يمنع الجسر تمرير البيانات إذا كانت موجهة من الجهاز أ إلى الجهاز ب

شكل ٨–٣ حركة نقل البيانات باستخدام الجسر

إذا استخدمت وحدة توصيل **hub** بدلاً من الجسر فسيكون تدفق البيانات للشبكة على جانبى الجسر مما يزيد من التصادمات والتنازع على الأجهزة . يسمح الجسر بأن يكون لديك مستويات وحدات توصيل إضافية فوق القيد الخاص بوحدات التوصيل الأربعة المفروض على شبكات ايثرنت.

والسؤال الآن متى تستخدم المبدل بدلا من وحدة التوصيل؟

والجواب فى حالتين. الأولى عندما يصل تدفق البيانات على الشبكة إلى مستوى تبدأ عنده التصادمات فى إبطاء الشبكة. والثانية إذا كنت تحتاج إلى أربعة مستويات من وحدات التوصيل فى شبكة اتصال**10 Base-T** أو أكثر من مستويين فى شبكة **100 Base-T**.

***الموجهات* (Routers)**

- تستخدم الموجهات مثل الجسور لتقسيم الشبكة إلى مقاطع والربط بينها ولكن بمستويً أعلى من التعقيد. تستخدم الموجهات للاتصال بالانترنت وداخل الانترنت، كما تستخدم كذلك لتوصيل شبكة واسعة **WAN** بشبكة محلية **LAN** . يشتمل الموجه على ذاكرة ومعالج (ولهذا يعتبر جهازا ذكيا). يساعده ذلك على فك تحزيم كل إطار يأتى إليه، ويلقى نظرة على كل حزم بيانات داخل الإطار، ثم يفحص عدد مرات دوران حزم البيانات فى

شبكة الاتصال، وينظر إلى عنوان الوجهة المنطقى ويحدد أفضل مسار للوصول إلى هناك. بعد ذلك يعيد تحزيم حزم البيانات فى إطار جديد باستخدام العنوان المادى الجديد، ويقوم بإرسال الإطار إلى وجهته.

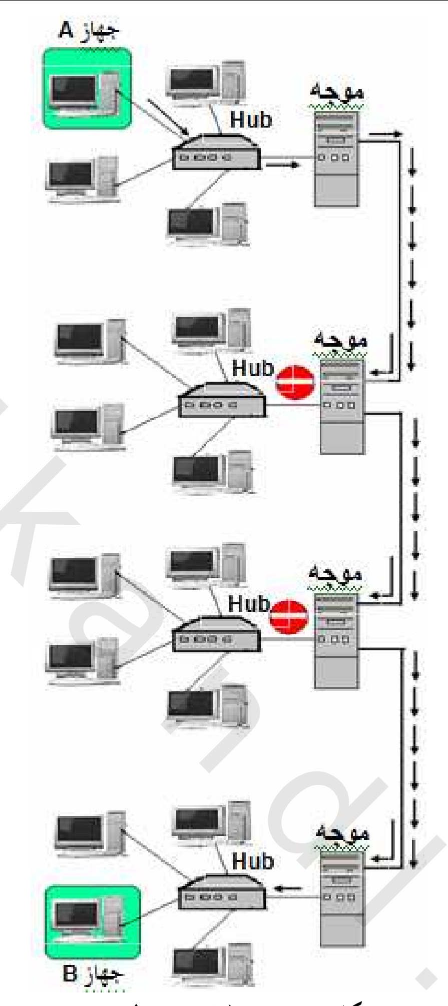
يعمل الموجه على طبقة الشبكة فى نموذج OSI. ولأن كل شبكة لها عنوان مميز، فإن الموجه يستعين بالمعلومات التى ينشئها البروتوكولIP لتحقيق هدفه.

يربط الموجه الشبكات المحلية التى تستخدم نفس بروتوكول طبقة الشبكة، حتى ولو استخدمت هذه الشبكات تقنيات وبروتوكولات مختلفة فى طبقة ربط البيانات. وهذا معناه أن الموجه يمكنه الربط بين شبكة تستخدم تقنية 100 BASE-T وشبكة أخرى تستخدم تقنية 100 BASE-F

كيف يعمل الموجه

يستخدم الموجه للربط بين شبكتين محليتين أو بين شبكة وموجه آخر متصل بشبكة أخرى. يشتمل الموجه على جداول تسمى جداول التوجيه. تحتوى جداول التوجيه على معلومات عن الشبكة المحيطة بها. ومن خلال هذه الجداول يقرر الموجه إرسال حزمة البيانات إلى جهاز متصل بالشبكة المجاورة له، أو إرسالها إلى موجه آخر وتفصيل ذلك على النحو التالى إذا أراد جهاز موجود على إحدى الشبكات الاتصال بجهاز موجود على شبكة محلية أخرى، فإن الجهاز يرسل بياناته إلى موجه الشبكة المحلية، والذى بدوره يرسل هذه البيانات إلى الشبكة المقصودة فى حالة ما إذا كان جهاز الوجهة موجودا على هذه الشبكة، وكانت هذه الشبكة موصلة مباشرة بالموجه. أما إذا كان جهاز الوجهة موجودا على شبكة أخرى فإن بيانات الجهاز المرسل تتجه إلى موجه آخر.

ويقوم الموجه الثانى بنفس العملية التى قام بها الموجه الأول، يعنى إرسال البيانات إلى جهاز آخر مشبوك على شبكة ، أو توجهها إلى موجه آخر، وهكذا تستمر العملية إلى أن تصل البيانات إلى وجهتها الأخيرة (انظر شكل ٨–٤)



شكل ٨–٤ عملية توجيه البيانات

فى شكل ٨–٤ يريد الجهاز A إرسال بيانات إلى جهاز B الموجود على شبكة محلية أخرى. أرسل الجهاز A بياناته إلى الموجه المتصل بشبكه والذى بدوره أرسلها إلى موجه آخر والموجه الأخير أرسلها إلى موجه ثالث والموجه الثالث أرسلها إلى موجه رابع وهذا الأخير أرسلها إلى الشبكة المحلية الموصلة معه والتى قامت بتوجيه البيانات إلى الجهاز B المتصل بها.

تسمى الشبكات التى يربطها الموجه مع بعضها بالشبكات الجامعة **Internetwork** ،

وتعتبر شبكة الإنترنت نموذج لشبكة جامعة تتكون من عدد كبير من الشبكات متصلة مع بعضها بواسطة موجهات.

ومن أهم مزايا استخدام الموجه ما يلي :

- تتحدث الموجهات إلى موجهات أخرى لتحديد أفضل مسار ولتتبع مسار الموجهات التى فشلت.
- تعمل الموجهات بسرعات عاليه جدا فتستطيع معالجة مابين ٢٥٠,٠٠٠حزمة بيانات إلى عدة ملايين فى الثانية الواحدة
- تقوم الموجهات بربط أنواع مختلفة من شبكات الاتصال، مثلا **100 Base F** و**100 BaseT**.

بطاقة الشبكة (NIC)

بطاقة الشبكة **(Network Interface Card)** وتختصر هكذا **NIC** . من أهم الأجهزة التى تلزمك لربط الشبكات ويطلق عليها أيضاً محول الشبكة (**LAN Adapter**) يحتاج ربط الشبكات فى أجهزة الكمبيوتر إلى كابل لربط جهازى كمبيوتر معاً ويحتاج إلى بطاقتى شبكة، يتم توصيلهما بجهازى الكمبيوتر لتوصيل الكابل بهما. باقى أجهـــزة ربـــط الشبكات تحتاج إليها حسب نوع الشبكة وإمكانيتها. كأن تتعدى نطاق جهازى كمبيوتر. لذلك تعد بطاقة الشبكة واحدة من الأجهزة المهمة ضمن أجهزة ربط الشبكات. تركـــب بطاقة الشبكة في إحدي فتحات التوسعة (**Expansion Slot**) في الجهاز وتثبت في شق من نوع **PCI** نوضح فيما يلى بعض الاعتبارات المهمة التى يجب أخذها فى الاعتبار عنـــد اتخاذ قرار شراء بطاقة الشبكة:

- نوع الناقل الذى ستستخدمه البطاقة.
- نوع بطاقة الشبكة.
- الماركة أو الشركة المصنعة للبطاقة.
- المميزات الإضافية التى تشتمل عليها البطاقة.

نوع الناقل الذي ستستخدمه الشبكة

نقصد بنوع ناقل بطاقة الشبكة هنا هل البطاقة سيتم تثبيتها فى فتحه **ISA** أم فى فتحة **PCI** . تستخدم معظم البطاقات فى الوقت الحالى ناقل **PCI** حيث أن الناقل **ISA** يعتبر تكنولوجيا قديمة. (انظر شكل ٨–٥)



شكل ٨–٥ صورة بطاقة الشبكة (**NIC**) من نوع **PCI**

ربما لم يعد لديك اختيار بشأن الناقل الذى تستخدمه فى أجهزة الكمبيوتر التى تقوم بإضافتها إلى شبكة الاتصال. حيث لم يعد الناقل **ISA** مستخدما لحظة إعداد هذا الكتاب. وأصبح خيارك الوحيد هو **PCI** ففي حين يبلغ اتساع فتحات **PCI** إلي ٣٢ بت، فإن اتساع فتحات **ISA** إما ٨ أو ١٦ بت ولأن بطاقة الشبكة تستخدم ١٦ بت فيظهر لك أن خيار **PCI** يكاد يكون هو الوحيد. تصل سرعة نقل البيانات مع ناقل **PCI** إلي ١٣٣ ميجابت في الثانية (**133 Mbps**) .

نوع بطاقة الشبكة

يجب أن تعرف هل بطاقة الشبكة تامة الازدواج أم نصف مزدوجة ؟ وهل بطاقة الشبكة تم تصنيعها من أجل وحدة خدمة أم لا ؟ وأخيرا هل البطاقة متعددة المنافذ أم لا.

البطاقة تامة الازدواج ونصف المزدوجة:البطاقة المزدوجة **(Full-duplex)** تستطيع الإرسال والاستقبال فى نفس الوقت. أما البطاقة نصف المزدوجة **(Half-duplex)**، فهى البطاقة التى تستطيع أن تستقبل فقط أو ترسل فقط. يعنى أنها لا تستطيع الإرسال

والاستقبال فى نفس الوقت. وطبيعى أن الازدواج يكون أسرع، مع أنه لا يضاعف السرعة لن تجد فى الأسواق هذه الأيام البطاقات نصف المزدوجة، لأن معظم بطاقات الشبكة **10/100** تامة الازدواج.

بطاقة شبكة وحدة الخدمة: تم تطوير بطاقات شبكة لتستخدم خصيصا لوحدة الخدمة. تتميز هذه البطاقة بأنها بطاقة ذكية ويمكن الاعتماد عليها. والبطاقة الذكية عبارة عن بطاقة تشتمل على معالج وذاكرة خاصة بها، وهذا الأمر يوفر لها سرعة عالية لأنها لا تضطر للخروج إلى المعالج والذاكرة الخاصة بالكمبيوتر. وطبعا ستنعكس سرعة بطاقة الشبكة على سرعة معالجة البيانات.

ماركة البطاقة أو الشركة المصنعة للبطاقة

ابحث عن بطاقة ذات علامة تجارية جيدة مثل **Intel** أو **3 Com**. مثل هذه البطاقات ستشمل على المميزات الخاصة التى تحدثنا عنها. فإذا لم يتيسر لك إحدى هذه العلامات التجارية، ابحث عن علامة تجارية مشهورة. كلما كانت البطاقة تحمل علامة تجارية مشهورة أو مميزة سيكون سعرها أعلى من البطاقات العامة التى لا تشتمل على مميزات خاصة.

لاشك أن التكلفة عنصر مهم عند الشراء ولكن فرق السعر سيكون أقل بكثير عندما تتعرض لمشكلة نتيجة لشراء بطاقات عامة أو لا تحمل علامة تجارية جيدة.

المميزات الإضافية التى تعتمد عليها بطاقة الشبكة

أهم المميزات الإضافية التى تشتمل عليها بطاقة الشبكة والتى تؤثر فى قرار الشراء هى ميزة إيقاظ الكمبيوتر **(Woke On LAN)**. تسمح هذه الميزة لبطاقة الشبكة بوضع الكمبيوتر فى وضع التشغيل الكامل بعد أن يتم إيقافه. الميزة الثانية هى ميزة بدء التشغيل عن بعد للخادم وهى تسمح ببدء تشغيل الكمبيوتر دون الاعتماد على نظام التشغيل المثبت على الكمبيوتر والميزة الثالثة من المميزات الإضافية لبطاقة الشبكة هى ميزة الإدارة عن بعد وهى تسمح لمدير شبكة الاتصال بمراقبة النشاط على وحدة خدمة بها البرنامج المناسب. لابد أن تكون اللوحة الأم تدعم هذه الميزات. اطمئن اللوحات الأم الحديثة كلها تدعم هذه الميزات.

نوضح فيما يلى بعض المعلومات التى تهمك عن عمل بطاقة الشبكة

- تزيد سرعة نقل البيانات من ذاكرة الجهاز إلى بطاقة الشبكة عن سرعة نقل البيانات من البطاقة إلى كابل الشبكة بفارق كبير، هذا الوضع يتطلب تخزين جزء من البيانات مؤقتا على ذاكرة بطاقة الشبكة. إلى أن تتمكن البطاقة من بثها إلى السلك. تسمى عملية التخزين المؤقتة هذه **Buffering** "التخزين المؤقت". يستخدم نفس المفهوم فى حالة استقبال البيانات فيتم تخزين البيانات التى تصل من قبل الشبكة مؤقتا إلى أن يصبح لدينا إطار بيانات كامل وجاهز للمعالجة من قبل طبقة ربط البيانات.
- تنتقل البيانات فى ممرات سعتها ١٦ بت أو ٣٢ بت أو ٦٤ بت فى المرة الواحدة، وتنتقل بشكل متوازٍ **(Parallel)** أما سلك الشبكة فلا يستطيع حمل أكثر من بت واحدة فى المرة الواحدة. فى عملية يطلق عليها البث المتسلسل **Serial Transmission**.

تقوم بطاقة الشبكة بتحويل البيانات من الجريان بشكل متوازٍ على ناقل البيانات داخل الجهاز، إلى الجريان بشكل متسلسل على كابل الشبكة وفى حالة الاستقبال تقوم بعملية عكسية أى التحويل من الشكل المتسلسل للبيانات إلى الشكل المتوازى.

أنواع الكابلات ومواصفاتها

الكابلات واحدة من الأجزاء المهمة داخل الشبكة فإذا لم يتم تركيب السلك الذي يربط الأجهزة بطريقة صحيحة، فلن تعمل الشبكة بطريقة صحيحة.

تستخدم تقنيات ربط الشبكات أحد أنواع الكابلات الآتية:

- كابل محورى رفيع **(Thin Coax)** ويستخدم مع **10Base2**.
- كابل مزدوج مجدول غير محمى **(UTP)** ويستخدم مع كل من **10Base T** و**100BaseT**.
- كابل ألياف بصرية ويستخدم مع كل من **10Base F**و**100Base F**.

نشرح فيما يلي أنواع كابلات الشبكات الثلاثة المستخدمة لربط الأجهزة داخل الشبكة .

الكابلات المحورية الرفيعة Coaxial Cables

يستخدم الكابل المحوري في تخطيط **Ethernet 10Base 2** يطلق علي هذا الكابل اسم **ThinNet** أو كابل **BNC** إشارة إلي نوع الموصل المستخدم عند طرفيه. وهو اختيار قديم لا ننصح باستخدامه إلا إذا لم يكن لديك خيار آخر، ولأن الكابل المحوري يمر من جهاز لآخر فإنه لا يحتاج إلي وحدة توصيل (**HUB**) . يمكن للكابل المحوري ربط حتى **255** جهاز بمقطع واحد وإن كنا لا نوصي بربط كل هذا العدد حيث يجب ألا يزيد أقصي طول للمقطع عن ١٨٥مترا.

يتكون الكابل من سلك داخلى، محاط بعازل بلاستيكى، مغطى بموصل خارجى معدنى مضفر،وأخيرا غلاف خارجى بلاستيكى كما يظهر شكل ٨-٦.

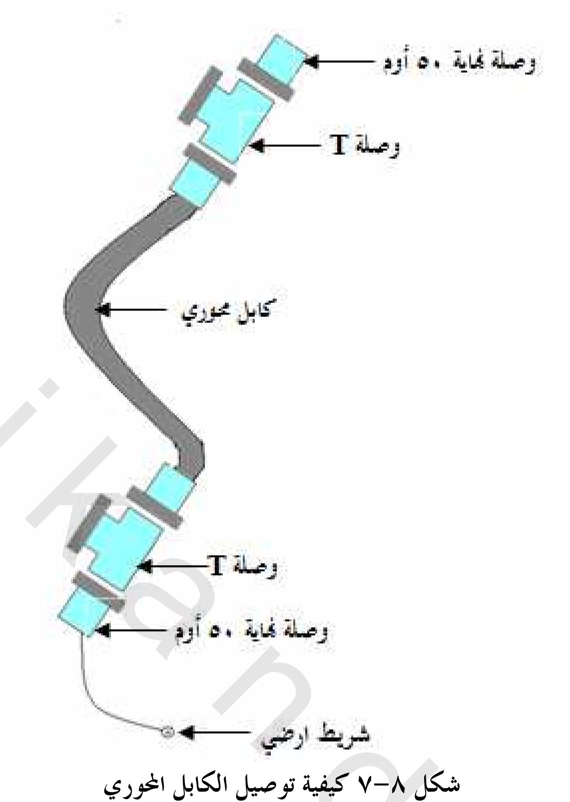


شكل ٨-٦ مقطع من الكابل المحوري

هناك عدة أنواع من الكابلات المحورية أشهرها **RG-58** وهو الكابل المحورى الرفيع المستخدم مع شبكات**Ethernet 10Base 2** وله مقاومة تبلغ ٥٠ أوم.

توصيل الكابل المحورى

يستخدم الكابل المحورى الرفيع موصلات يطلق عليها **BNC** يتم تدويرها لربطها على كل طرف من الكابل وتتصل ببطاقة الشبكة باستخدام وصلة **T** كما يتضح من شكل ٨-٧



شكل ٨–٧ كيفية توصيل الكابل المحوري

تشكل أجهزة الكمبيوتر المرتبطة بهذه الطريقة خطا طويلا يسمى تخطيط الناقل **(Bus Topology)**.عند كل طرف من شبكة الاتصال توجد وصلة نهاية **(Terminator)** ٥٠ أوم وتحتاج واحدة فقط من وصلات النهاية إلى توصيلها أرضيا عن طريق ربطها بمسمار على صندوق الكمبيوتر المتصل بها. كما يتضح من الشكل السابق

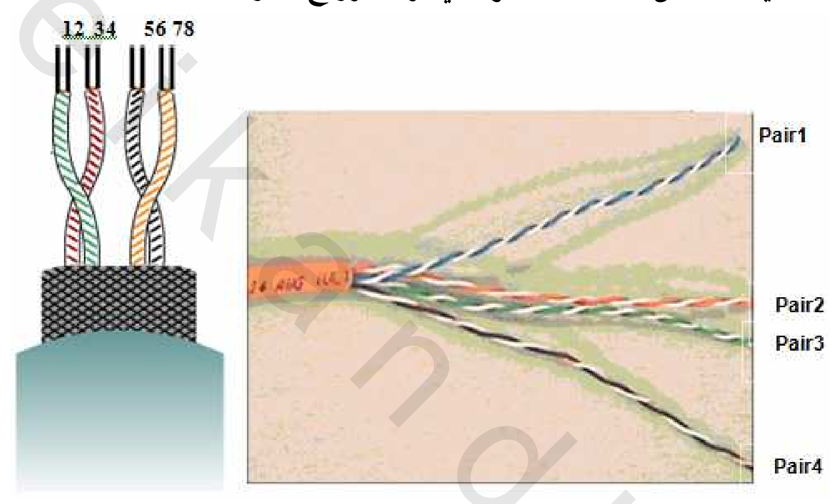
يعد الكابل المحورى الرفيع أصعب فى التعامل معه رغم أنه لا يعتبر رخيص بالمقارنة بالأنواع الأخرى. يجب أن تسترشد بشخص ذو خبرة بنوعية الكابلات إذا لم تكن لديك هذه الخبرة.

***الزوج المجدول غير المحمي* Unshielded Twisted-Pair**

يعد هذا الكابل الأكثر شيوعا لربط الشبكات ويسمي **Unshielded Twisted Pair** وتختصر هكذا **UTP**. والسبب فى جدل الأسلاك فى كابل **UTP** حول

بعضها تقليل التشوش الكهربى الذي يمكن أن يلتقطه الكابل.

أسلاك الزوج المجدول غير المحمي (UTP) المستخدمة لربط الشبكات أسلاك من ثمانية موصلات نحاسية وأربعة أزواج تشبه الأسلاك المستخدمة عند توصيل الهاتف بالمنازل. الفرق بين هذه الأسلاك وأسلاك الهاتف أن أسلاك الهاتف لها زوجان من الأسلاك (أربعة أسلاك) بينما لأسلاك UTP أربعة أزواج (أي ثمانية أسلاك). يوضح شكل ٨-٨ كابل UTP الذي يتألف من ثمانية أسلاك مرتبة في أربعة أزواج مجدولة



شكل ٨-٨ أزواج كابل الـــ UTP

يتم جدل الأسلاك أولا فى أزواج ثم يتم جدل الأزواج مع بعضها ويتم وضع وصلة RJ-45 عند كل طرف من الكابل. تشبه وصلة RJ-45 التى تتعامل مع أربعة أزواج مجدولة من الأسلاك، وصلة RJ-11 التى يمكنها التعامل مع زوجين من الأسلاك ويتم اســتخدامها فى وصلة الهاتف العادية، ولكنها أكبر منها قليلا. يستخدم 100 Base-T و1000 Base-T أربعة أو ثمانية أزواج من الأسلاك فى كابل من نوع Category 5 ونفس وصلة RJ-45 .

دائما نقول الكابل المزدوج غير المحمى. فهل هناك كابل مزدوج محمى؟ وللإجابة على هذا السؤال نقول نعم. يعد الكابل المزدوج المحمى STP مأخوذة مـــن عبـــارة (Shielded Twisted Pair) بديلا للكابل المزدوج غير المحمى، وله درجات مختلفة من الحماية . حماية حول كل زوج من الأسلاك ، أو حماية حول الزوجين ، أو حماية حول الـــزوجين بـــصفة

مستقلة وحول الأسلاك كلها . ولكنه أكثر تكلفة وأكثر صعوبة في التعامل من كابلUTP.

فئات UTP

تأتي الأسلاك المزدوجة المجدولة في ٦ فئات (**Categories**) لكل فئة استخدام . ننصح بتركيب كابلات نحاسية لا تقل عن الفئة **(Category 5)** تسمي **CAT 5** لأن هذا النوع يطيل عمر الشبكة.فيما يلى نوضح فئات **UTP** الستة واستخداماها :

- الفئه١ **(Category1)**: كانت تستخدم فى تركيبات الهاتف ولذلك لايتم تقديرها وفقا للأداء.
- الفئه٢ **(Category 2)**: تستخدم أيضا فى تركيبات الهاتف واستخدمت فى شبكات الاتصال الأولى.
- الفئه٣ **(Category3)**: تحتوى على أربعة أزواج من الأسلاك المجدولة. وتعتبر أقل مستوى يمكن استخدامه لربط الشبكات. وتستخدم من اجل شبكات **10Base 2 Ethernet**. ويبلغ أقصى معدل بيانات لها ١٦ميجابت/ثانيه.
- الفئة٤ **(Category 4)**: تحتوى هذه الفئة على أربعة أزواج من الأسلاك المجدولة ويبلغ أقصى معدل بيانات لها ٢٠ميجابت/ثانية. تستخدم مع شبكات **Token Ring** و **Ethernet 10Base T** .
- الفئة٥ **(Category5)**: تستخدم مع شبكات **Ethernet 100 Base-T** ويبلغ أقصى معدل بيانات لها **100** ميجابت/ثانية . تحتوي علي أربعة أزواج من الأسلاك المجدولة . تعد هذه الفئة من أكثر الكابلات شيوعاً في الوقت الحالي .لا تستخدم كابل أقل من **Category 5** في شبكتك .
- الفئه٥إى **(Category 5e)**:لها نفس خصائص الفئة ٥ بمعدل خطأ أقل. تشير **e** إلي **Enhanced** يعني مطور .
- الفئه٦ **(Category 6)**:تستخدم مع شبكات جيجابت ايثرنت **(Gigabit Ethernet)**.ويبلغ أقصى معدل بيانات لها ٣٥٠ ميجابت/ثانية. تحتوي هذه الفئة علي أربعة أزواج من الأسلاك المجدولة بغلاف من الرقائق المعدنية حول كل زوج ، وغلاف آخر

من الرقائق المعدنية حول كل الأزواج .

ننصح أيضا ألا توفر في الكابلات لأن ثمن الكابلات عموما بالنسبة لأجهزة الشبكة رخـيص والتكلفة في التركيب، علي سبيل المثال تبلغ أقصي مسافة لشبكة Ethernet 10Base-T باستخدام أسلاك مزدوجة مجدولة ١٠٠ متر بين جهاز HUB وجهاز الكمبيوتر، بينما تبلغ أقصي مسافة لشبكة Ethernet 100Base-T ٢٠ متر بين كل محطة والتي تليها.

يعتبر كابل UTP هو الكابل القياسي في هذه الأيام وننصح باستخدامه لأنه سهل التركيـب وتكلفته معقولة وسهل الصيانة .

***معيار توصيل أسلاك* UTP**

يستخدم المعيار EIA 568B لتوصيل كابلات UTP. للحفاظ على أقصى معدل للبيانات يجب معالجة الأسلاك وإنهاؤها أو توصيلها وفقا لمعيار EIA 568B.

يوضح الجدول التالي الترتيب الذي يجب إنهاء الأسلاك به (عند رؤيتها من الأعلى) وفقا لمقياس EIA 568B. إذا لم يتم إنهاء الأسلاك بحسب الترتيب الوارد بالجدول عنـد كـل طرف من الكابل لن ترسل البيانات بصورة صحيحة.

الإبرة Pin	لون السلك
١	أبيض وبرتقالى
٢	برتقالى
٣	أبيض وأخضر
٤	أزرق
٥	أبيض وأزرق
٦	أخضر
٧	أبيض وبنى
٨	بنى

تلاحظ من الجدول أن لون الإبر الفردية يكون دائما أبيض ممزوجا بلون آخر.

ربط الموصلات بالكابل

إن أصعب جزء في تثبيت كابلات الشبكة هو ربط الموصلات بالكابل. لذا، من أسهل وسائل تثبيت الكابلات شراء كابلات محددة الأطوال ومتصلة بالموصلات بالفعل. تباع كابلات **Thin Net Coax** أو **Coax** بالأطوال المحددة التالية: **25** و**50** و**100** قدم. كما يمكن شراء كابلات **Twisted-Pair** محددة الطول أيضاً، أو ربط الموصلات بالكابلات بنفسك إذا كان لديك القدرة على القيام بذلك والتغلب على الصعوبات المتضمنة في هذه العملية.

قبل التحدث عن كيفية ربط الموصلات بالكابل، فيما يلي بعض الإرشادات العامة عن استخدام الكابلات:

- استخدام أطوال من الكابلات تزيد عن الأطوال التي تحتاج إليها في شبكتك، خاصة إذا كنت ستمدها عبر الحوائط.
- حاول عند مد الكابلات أن تتجنب قدر الإمكان كل ما قد يؤدي إلى تداخل الإشارات، مثل مصابيح الفلورسنت والموتورات الكبرى وما إلى ذلك. تعد مصابيح الفلورسنت أكثر المصادر التي ينشأ عنها تداخل الإشارات. من الأفضل ألا تقل المسافة الفاصلة بين الكابلات ومصابيح الفلورسنت عن ثلاثة أقدام.
- في حالة مد الكابلات عبر الأرض، قم بتغطيتها حتى لا يتعثر فيها أحد. يمكن أن تجد أغلفة واقية للكابلات بأسعار مناسبة في المحلات المتخصصة في الأدوات الكهربية .
- عند مد الكابلات عبر الحائط، أحرص على تعليم طرفي كل كابل، يمكنك أن تستعين في ذلك بلصق بطاقات مختلفة الحروف والأرقام عند طرف كل كابل.
- عندما يتجمع أكثر من كابل في نفس الموضع، قم بربطها جميعاً معاً باستخدام رابط كابلات بلاستيكي. تجنب استخدام الورق اللاصق قدر الإمكان، فإنه يفسد سريعاً.
- عند مد الكابلات فوق أجزاء أسقف جاهزة، استخدم روابط كابلات أو صواميل لتثبيت الكابل بالسقف الفعلي أو بالإطار المعدني الذي يدعم أجزاء السقف الجاهز. لا تلقي الكابلات على أجزاء السقف.

الأدوات المطلوبة

لابد أن تتوافر لديك الأدوات المطلوبة حتى يتم تثبيت الكابلات على الوجه الأمثل.

في البداية، يجب أن تكون لديك مجموعة من الأدوات الرئيسية للعمل على أجهزة الكمبيوتر، والتي يمكن شراؤها بسعر مناسب من أي محل لبيع مكونات أجهزة الكمبيوتر أو تجهيزات المكاتب. تتضمن هذه الأدوات مفكات ومفاتيح ربط أنبوبية الشكل لفتح أجهزة الكمبيوتر وإدراج كروت الشبكة. (إذا لم تكن لديك هذه الأدوات، فيجب أن يكون لديك على الأقل مفكات **Phillips** أو **Flat-Head** "مسطحة الرأس" بأحجام مختلفة).

إذا كانت جميع أجهزة الكمبيوتر تقع في نفس الحجرة وكنت ترغب في مد الكابلات عبر الأرضية وكانت الكابلات التي تستخدمها محددة الطول مسبقاً، فلن تحتاج إلى استخدام أدوات أخرى.

إذا كنت تستخدم كابلات غير محددة الطول وترغب في ربطها بالموصلات بنفسك، فسوف تحتاج إلى الأدوات التالية بالإضافة إلى أدوات الكمبيوتر الرئيسية السابقة:

- لاوية **Crimper** : وهي عبارة عن أداة تتضمن مجموعة من اللقم اللولبية تمكن من عصر جزئي **RJ-45** مع بعضها وبداخلهما الأسلاك
- قاطعات أسلاك: سوف تحتاج إلى قاطعات كبيرة الحجم لكابلات **Coax** ويمكن أن تستخدم قاطعات صغيرة مع كابل **10baseT**.
- مكبس مناسب لنوع الكابل لربط الموصلات بالكابل.
- مجزئ الكابل: لن تحتاج إلى هذه الأداة إلا في حالة عدم احتواء المكبس عليها. يجب استخدام مجزئ الكابل مع كابلات **Coax** على وجه الخصوص لقطع الناقل الداخلي والخارجي والمادة العازلة الخارجية بنفس الأطوال.
- أداة تجريد العازل: لتقشير العازل من الكابل

إذا كنت ترغب في مد الكابلات عبر الحائط، فهناك أدوات مختلفة سوف تحتاج إليها هذه الأدوات هي:

- مطرقة
- مثقاب
- كشاف كهربي
- سلم
- مواسير داخل الحائط. يتم دفع الماسورة إلى فتحة في الحائط وجذبها إلى فتحة أخرى حيث يثبت الكابل بداخلها.

إذا كنت ترغب في مد الكابلات عبر أعمدة مسلحة فسوف تحتاج إلى ثقابة تعمل بالهواء المضغوط.

ربط موصل RJ-45 بكابل UTP

يتسم ربط موصلات **RJ-45** بكابلات **UTP** بقدر أكبر من السهولة من ربط موصلات **BNC** بكابلات **Coax** أهم خطوة في هذه العملية هي توصيل كل سلك بـ **Pin** (الإبرة) المناسبة (كما هو موضح بالجدول السابق) .

مثلاً تتطلب الشبكات العاملة بمعيار **100Base-T** استخدام كابل مكون من أربعة أزواج من الأسلاك مع ربط جميع الأسلاك الثمانية بالموصل.

فيما يلي كيفية ربط الموصل بالكابل:

١. قم بقطع طرف الكابل بحيث تحصل على الطول المطلوب، مع مراعاة القطع في وضع مستقيم وليس مائل.
٢. قم بتجريد قليل من العازل عن الكابل.
٣. رتب الأسلاك حسب المعيار الذي اخترت استخدامه .
٤. ضع الأسلاك داخل الوصلة.
٥. ضع الوصلة مع الأسلاك في المكان المخصص لها في اللاوية ،
٦. قم بإدراج الموصل بالأسلاك في جزء المكبس في اللاوية ثم اضغط على المقابض لضغط الموصل، وعصر الأسلاك.

أخرج الموصل من الأداة وتأكد من سلامة الربط.

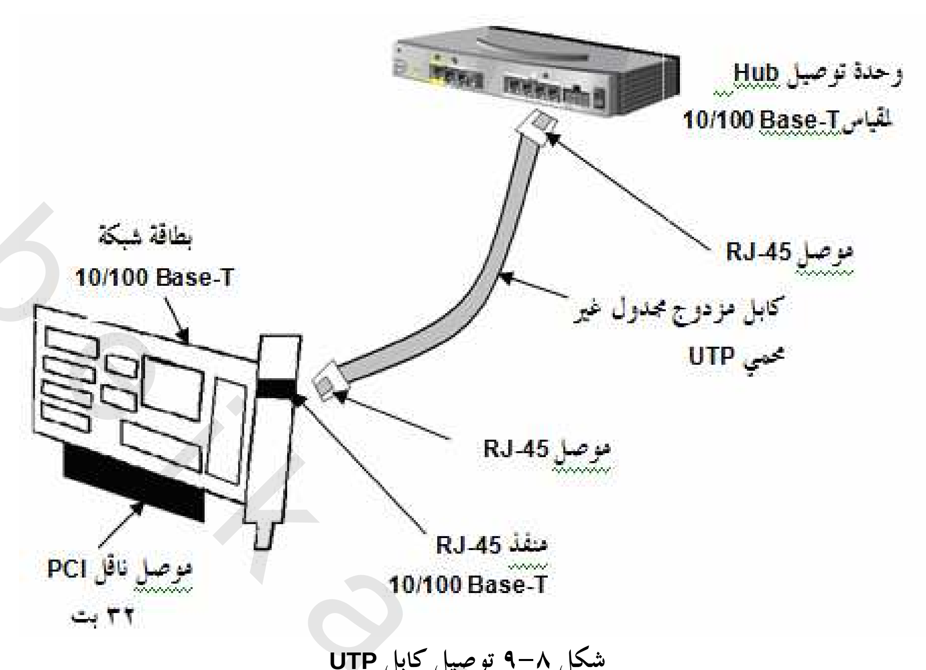
بعد ذلك أعد الخطوات من ١ إلى ٦ مع الطرف الثاني من الكابل. وبهذا يكون الكابل جاهزاً لتوصيل جهاز الكمبيوتر بالـ hub .

فيما يلي بعض النقاط الواجب الانتباه إليها عند ربط موصلات RJ-45 بكابل UTP

- **لا ترقم Pins في موصلات RJ-45 ولكن عند الإمساك بالموصل بحيث تكون الناقلات المعدنية متجهة لأعلى، كما هو موضح في شكل (٨-٩) السابق ، يكون Pin1 على اليسار.**
- **في حالة تثبيت الكابل في شبكة Fast Ethernet ، احرص على إتباع قواعد تثبيت كابلات Category-5. وبالطبع، يجب أن تكون جميع المكونات المستخدمة كالكابلات والموصلات، من Category-5.**
- **عند ربط الموصل، لا تقم بتقشير أكثر من نصف بوصة من الكابل ولا تزيد أجزاء الكابل عن الحد الأقصى المحدد (100متر). إذا لم تكن متيقناً من قدرتك على مراعاة ذلك ، فالجأ إلى أحد المتخصصين .**

توصيل كابل UTP

يتم توصيل كابل UTP فى بطاقة الشبكة ثم فى منفذ حائطى أو وحدة توصيل(hub) مما يجعل تركيب شبكة 10/100 Base – T سهلاً للغاية (انظر شكل ٨-٩) . عندما يتصل جهازا كمبيوتر ببعضهما مباشرة بدون وحدة توصيل (Hub) ، يجب استخدام كابل خاص له وصلات طرفية معكوسة .



شكل ٨–٩ توصيل كابل **UTP**

يجب أن تصبح كابلات النقل علي أحد جهازي الكمبيوتر ، هي كابلات استقبال علـي الجهاز الآخر .

معالجة مشكلة التشويش

لمعالجة مشكلة التشويش هناك قواعد عديدة يجب إتباعها عند تمرير الكابل:

- **يفضل مد الكابلات عبر الأسقف والحوائط وليس الأرضية، كما يفضل تركيب jack على الحائط بجوار كل جهاز كمبيوتر يتصل بالجهاز المجاور له بكابل توصيل قصير (يبلغ طولـه 10 قدم أو ما شابه ذلك). احرص على استخدام Jacks من Category-5 ذات أعلى جودة ممكنة وتأكد من التفاف كل زوج من الأسلاك داخل الكابل حتى نقطة اتصاله بـ Jack. بمعنى آخر، لا تقم بفك الأسلاك زيادة عن القدر الذي يتيح العمل باسـتخدامها بسهولة.**
- **عند مد الأسلاك عبر الحوائط والأسقف، احرص على تجنب أسلاك الكهرباء ومـصابيح الفلورسنت وغيرها من الأجهزة الكهربائية الـتي قـد تـؤدي إلى تـداخل الإشـارات**

الكهرومغناطيسية مع الإشارات المارة في الكابل. لا تقم بطي الكابل ولكن اجعله ينحني مع الأركان.

نصائح هامة

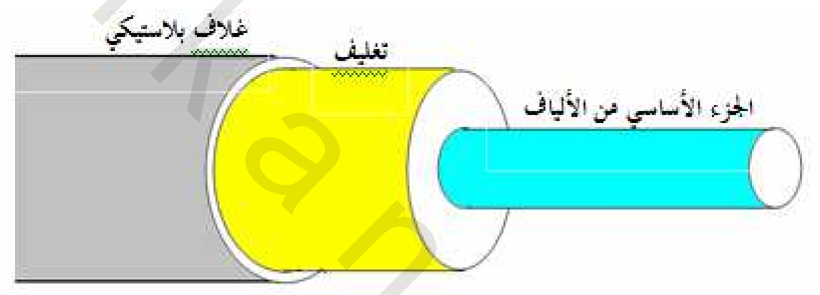
- **من الأفضل أن تمد كابل إلى كل موضع محتمل لأجهزة الكمبيوتر، وإن لم يكن لديك حالياً جهاز ترغب في وضعه في هذا الموضع. بهذا، إذا أردت أن تنقل جهاز من مكان لآخر، فلن تحتاج إلى مد المزيد من الأسلاك. وما عليك في هذه الحالة سوى وصله بـ jack في الحائط من خلال كابل التوصيل.**
- **خصص ركن من مخزن أو حجرة احتياطية لكي يكون صندوق الأسلاك التي تتجمع فيه كابلات الشبكة. اجمع الكابلات معاً واربطها بوحدة توصيل مركزية وهي عبارة عن مجموعة RJ-45 jack مرتبة في صف واحد.**

الألياف البصرية Optical Fiber

النوع الثالث من كابلات الشبكة هو الألياف البصرية (Optical Fiber) وهي تعتبر غالية الثمن مقارنة بالكابلات السابقة. وتستخدم في الغالب من أجل ارتباطات عالية السرعة .من عيوب الكابلات النحاسية ضعف الإشارة المرسلة كلما بعدت المسافة .مثلاً تصبح الإشارة غير مقروءة بعد ١٠٠ متر في حالة كابل UTP وبعد ٥٠٠ متر في حالة شبكة 10 Base5 . أما بالنسبة للألياف البصرية فمن الممكن تمديد الكابل حتي طول ١٢٠ كيلومتر دون انخفاض ملحوظ في مستوي الإشارة . يناسب هذا النوع من الكابلات الأنظمة البعيدة عن بعضها . أما عن فكرة عمل الألياف البصرية فإنها تنقل بيانات الشبكة باستخدام نبضات من الضوء بدلا من النبضات الكهربية التي يتم إرسالها من الأسلاك النحاسية. ينقل كابل الألياف البصرية الضوء على ألياف من الزجاج ذات سمك أقل من سمك شعرة الرأس. يتم نقل المعلومات عن طريق تشغيل مصدر الضوء وإيقاف تشغيله لإنتاج أرقام واحد وصفر.عند الطرف الآخر من الكابل، توجد دائرة كاشفة للضوء، تقوم بتحويل الضوء مرة أخرى إلى نبضات كهربائية. من مزايا الكابلات الضوئية أنها تمنع التشويش الكهربائى والكهرومغناطيسى وهى وسيلة مؤمنة وكفئاً لحمل المعلومات بسرعة عبر مسافات طويلة.

تحتاج الألياف البصرية إلي فني ماهر نظرا لصعوبة تركيبها وصيانتها . ويعد إنهـــاء الأليـــاف الضوئية امرأ صعبا غير مأمون العواقب.

يتكون كابل الألياف البصرية كما يتضح من الشكل ٨–١٠ من جزء أساسى من الزجاج الشفاف (أو بلاستيك بالنسبة للمسافات القصيرة). يتمثل دوره فى نقل البيانات التى تكون عبارة عن نبضات ضوئية فى هذه الحالة. تتم إحاطة هذا الجزء بتغليف من زجاج عـــاكس يحافظ على بقاء النبضات الضوئية تنعكس إلى داخل الزجاج الشفاف بدلا من مغادرتـــه. (يعنى إعادة توجيه الضوء الصادر من الجزء الأساسى إليه مرة أخرى). وتتم تغطية التغليف بطبقة بلاستيكية واحدة أو أكثر ومواد مقوية أخرى لعمل غلاف.



شكل ٨–١٠ مقطع من كابل الألياف البصرية

أنواع الألياف البصرية

يوجد نوعان من كابلات الألياف البصرية وهما :

ألياف أحادية النمط

يتم استخدام الألياف أحادية النمط فى الشبكات الواسعة (WAN) ذات المسافات الطويلة وتستخدم بصورة أقل فى ربط شبكات الاتصال الموجودة فى مكان واحد، تحمل الألياف البصرية أحادية النمط الضوء إلى الألياف مباشرة. وتتميز بكفاءتها العاليـــة ممـــا يـــسمح باستخدامها لمسافات طويلة تعادل أضعاف مسافة الألياف متعددة النمط. ولكن تكلفتـــها تصل ضعف تكلفة الألياف متعددة الأنماط .

الألياف متعددة الأنماط.

حسب الشرح السابق تمتد الألياف متعددة الأنماط لمسافات أقل مـــن الأليـــاف

أحادية النمط وتكلفتها أقل. يستخدم هذا النوع من الألياف البصرية ثنائيا قاذفا للـــضوء LED كمنبع أو إشارة ضوئية حاملة للبيانات المرسلة .

مخلص الفصل

شرحنا بالتفصيل أجهزة التوصيل المستخدمة في الشبكات حيث بـــدأنا بـــشرح وحـــدة التوصيل (Hub) ثم شرحنا المبدلات (Switches) والجسور (Bridges) وأخيرا تحدثنا عن الموجهات (Routers) وأوضحنا متى يفضل أن تستخدم كل نوع من هذه الأجهزة. شرحنا بعد ذلك بطاقة الشبكة (NIC) وركزنا على الاعتبارات التي تفضل بطاقة شـــبكة على أخرى . شرحنا كذلك أنواع الكابلات المستخدمة لربط الـــشبكات وقـــسمناها إلى كابل محوري (Coax) رفيع وكابل مزدوج مجدول غير محمـــي وكابـــل أليـــاف بـــصرية وأوضحنا أنواع الشبكات التي تستخدم كل نوع من هذه الأنواع.شرحنا أيضا كيفية ربط الموصلات بالكابل وكيفية توصيل توصيل كابل UTP.

تدريبات

١. من الأسباب التي تجعلك تفضل استخدام رمز التبديل Switch بدلاً مـــن وحـــدة التوصيل HUB (اختر سببين فقط):

أ. في حالة الشبكات التي يزيد عليها تدفق البيانات، ويمكن أن يسبب التنازع علـــى تردد النطاق بطء الشبكة

ب. لأن رمز التبديل أرخص من وحدة التوصيل

ج. الشبكات التي يجب تجزئتها إلى مقاطع من أجل تحقيق مستوى أعلى من التـــأمين أو الأداء

د. رمز التبديل أقل تكلفة وأقل عرضة للأعطال من وحدة التوصيل

٢. صل الإجابة الصحيحة التي توضح وظيفة كل جهاز من الأجهزة التالية:

أ. وحدة التوصيل Hub ١. يستخدم لتقسيم الشبكة إلى مقاطع و يعمل على طبقة ربط البيانات في نموذج OSI .

ب. المبدل Switch ٢. يستخدم لربط شبكة محلـــة LAN بـــشبكة واســـعة

	WAN ويحتوي على ذاكرة ومعالج ويعمل علي طبقة الشبكة في نموذج OSI
ج. الجسر Bridge	٣. يرسل الإشارة إلى منفذ الوجهة فقط ويعمل علي الطبقة المادية في نموذج OSI
د. الموجه Router	٤. يبث الإشارة إلى كل المنافذ

٣. اختر الإجابة الصحيحة:

أ. عند استخدام Hub بدلاً من Switch (يزيد عدد التصادمات / يقل عدد التصادمات / لا يزيد ولا يقل عدد التصادمات)

ب. عند توصيل عدة شبكات محلية باستخدام موجهات نحصل على (شبكة الانترنت / شبكة جامعة)

ج. الجهاز الذي لا يقرأ طبقة ربط البيانات في الرزم الواردة هو (الموجه / الجسر / المبدل / وحدة التوصيل)

د. بطاقة الشبكة من نوع ISA (تدعم / لا تدعم) تقنية التركيب والتشغيل Plug and Play

هـ . نلجأ إلى مفهوم التخزين المؤقت (Caching) (لأن سرعة نقل البيانات في الجهاز أكبر من سرعة نقل البيانات على كابل الشبكة / لتشغيل البيانات عند الحاجة إليها)

٤. اذكر ثلاثة من الاعتبارات المهمة التي يجب أخذها في الاعتبار قبل اتخاذ قرار شراء بطاقة الشبكة

٥. ما هو الفرق الجوهري بين منافذ Hub ومنفذ الربط التوسعي؟

٦. يستخدم كابل UTP وصلات من نوع

أ. RJII

ب. RG58

ج. RJ45

٧. السبب في جدل الأسلاك في كابل UTP حول بعضها

أ. حماية الأسلاك من الانكسار

ب. توصيل الأسلاك الموجبة مع الأسلاك السالبة

ج. منع التشويش الذي يمكن أن يلتقطه الكابل

٨. صح أم خطأ

أ. يستخدم الكابل المحوري الرفيع (Coax) في تطبيقات الشبكات الحديثة مثل Ethernet 1000 BASE-T

ب. تستخدم أسلاك كابل UTP أربعة أزواج من الأسلاك (أي ثمانية أسلاك) بينما أسلاك الهاتف المنزلي زوجان من الأسلاك (أربعة أسلاك)

ج. الكابل المزدوج المحمي STP أكثر تكلفة وأكثر صعوبة في التعامل من كابل UTP

د. لا تنصح باستخدام كابل UTP لارتفاع تكلفتة وصعوبة تركيبة وصيانتة.

٩. السبب في استخدام الألياف البصرية:

أ. استخدام الكابلات لمسافات طويلة دون انخفاض ملحوظ في مستوى الإشارة

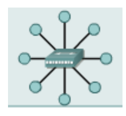
ب. أن تكلفتها رخيصة جداً بالمقارنة بالكابلات النحاسية

ج. ربط أجهزة قريبة من بعضها على مستوى شبكة محلية

د. كل ما سبق

هـ. لا شئ مما سبق

١٠. يوجد نوعين من الليف البصري هما .... و ....





تكلمنا عن وحدة الخدمة فى كثير من الفصول السابقة، ونظرا لأهمية وحدة الخدمة فى شبكة الاتصال فإننا نعود فى هذا الفصل للحديث عنها بشكل مستقل. بانتهاء هذا الفصل ستتعرف على:

- ***استخدام جهاز الكمبيوتر كوحدة خدمة***
- ***وحدة الخدمة المخصصة***
- ***مجموعات RAID***
- ***المبادلة الفعالة***

Server هو موضوع هذا الفصل . لهذه الكلمة ترجمات كثيرة البعض يترجمها (الخادم) والبعض الأخر يترجمها (الملقم). ولكنني سأعتمد فى هذا الكتاب ترجمتها بـــ "وحدة الخدمة". واحياناً "الخادم" حسب ما يقتضيه سياق الجملة سواء كان جهاز الكمبيوتر المستخدم كوحدة خدمة يعمل كجهاز تابع ووحدة خدمة فى نفس الوقت ، أو كان جهازا مستقلا يستخدم كوحدة خدمة مستقلة ، فانه يقوم بوظفية خدمة الأجهزة أو الوحدات التابعة فى الشبكة .

إما الأجهزة التابعة فإنها تسمى بـــ محطة عمل أو" وحـــدة عمـــل " أو بــــــ " **Work Station** الهدف من إيراد هذه الأسماء ومرادفاتها فى بداية الفصل ألا يحدث لديك لبس عندما تسمع أو تقرأ مرادفات هذه الكلمات فى كتب أخرى .

من هذا نفهم أن وحدة الخدمة عبارة عن جهاز كمبيوتر مثل أجهزة كمبيوتر سطح المكتب التي تعمل عليها. الاختلاف الأساسي بينه وبين جهاز سطح المكتب أن وحـــدة الخدمـــة "الجهاز الخادم" يشارك موارده مع أجهزة كمبيوتر أخري علي الشبكة . ويجب أن يلـــبي حاجة المستخدمين في نقل البيانات بسرعة والتأكد من أمان البيانات وتكاملها .

تستطيع وحدة الخدمة نقل البيانات خارج الأقراص وعبر أسلاك الشبكة بينما لا يستطيع جهاز كمبيوتر سطح المكتب ذلك .

عادة تكون وحدة الخدمة أكثر قوة من نظم سطح المكتب، بمعـــني أن ســـرعة المعـــالج والذاكرة تكون عادة أكبر، وأن كان ذلك ليس هو المقياس الوحيد لفائدة وحدة الخدمة، كما أن وحدة الخدمة توفر شكلا من التأمين ضد الكوارث لا توفره معظم أجهزة سطح المكتب.

الغاية من وحدة الخدمة أو الخادم أن يقوم بتمرير البيانات إلي وحـــدات تابعـــة متعـــددة بكفاءة، ولذلك فالخادم الذي لا يستطيع تمرير البيانات إلي باقي الوحدات بكفاءة يعد بطيئا حتي وإن كان يعمل بسرعة هائلة. ولذلك يعد نظام "الإدخال / الإخراج" **I/O** مهما جدا للخادم .

نتناول فى هذا الفصل بإذن الله شرح نوعين من وحدات الخدمة

الأول: وحدة الخدمة التي تعمل كجهاز تابع ووحدة خدمة فى نفس الوقت.

والثانى : وحدة الخدمة التي تعمل على جهاز كمبيوتر مستقل يعمل كوحدة خدمة مستقلة. سنوضح أيضا مزايا وعيوب كلا النوعين من وحدات الخدمة.

استخدام جهاز الكمبيوتر كوحدة خدمة

يجب تحويل الجهاز العامل بنظام **Windows** إلى وحدة خدمة لكي تتمكن الأجهزة الأخرى على الشبكة من استخدام الطابعة المتصلة بجهازك واى مجلدات أو ملفات تسمح بالمشاركة فيها وبهذا يكون الجهاز وحدة خدمة وجهاز تابع فى نفس الوقت .فيعمل كوحدة خدمة عندما يقوم مستخدم آخر بإرسال عمل للطباعة على طابعتك، أو الوصول إلى ملف مخزن على القرص الصلب بجهازك. ويعمل كجهاز تابع عندما تقوم بإرسال عمل إلى طابعة الشبكة أو عندما تقوم بالوصول إلى ملف مخزن على القرص الصلب لوحدة خدمة أخرى.

تمكين مشاركة الملفات والطابعة

لكي تتمكن من مشاركة الملفات أو الطابعة مع مستخدمي الشبكة، يجب أن تقوم بإعداد خاصية في **Windows** تعرف باسم **File and Printer Sharing** فبدونها لن يعمل جهازك كوحدة خدمة. قد تكون هذه الخاصية معدة بالفعل علي جهازك وفي هذه الحالة لن تفعل شيئا. أما إذا لم تكن خاصية **File and Printer Sharing** معدة علي جهازك، فيجب عليك في هذه الحالة تثبيتها حتي تتمكن من مشاركة ملف أو طابعة مع غيرك من مستخدمي الشبكة

اتبع الخطوات التالية لتثبيت هذه الخاصية علي جهاز يعمل بنظام **Windows Vista** في حالة عدم تثبيتها من قبل باعتباره أحدث نظم التشغيل حتي لحظة إعداد هذا الكتاب.

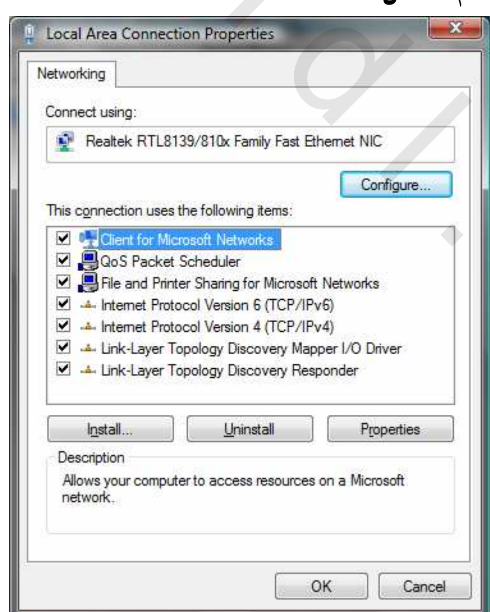
إذا كنت تعمل علي جهاز يعمل بنظام **Windows XP** أو إصدار آخر. استرشد بالخطوات الآتية في إعداد شبكتك حيث أنه لا توجد خطوات ثابتة في كل نظم التشغيل لمشاركة الملفات والطابعات والأقراص.

١. تأكد من دخولك إلي الجهاز بحساب مدير أو مسئول **Administrator**، انقر قائمة **Start** "ابدأ"، ثم اختر **Control Panel** ، ثم انقر الارتباط **Network and Internet** "الشبكة والانترنت" ثم انقر **Network and Sharing Center** "مركز الشبكة والمشاركة" .

٢. من قائمة المهام في الناحية اليسري من النافذة ، انقر الارتباط **Manage Network Connection** "إدارة اتصالات الشبكة".

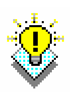
٣. بزر الماوس الأيمن انقر **Local Area Connection** ومن القائمة التي ستظهر اختر **Properties** "خصائص".

٤. عندما يظهر مربع **User Account Control** "التحكم في حساب المستخدم" إذا كنت مسجلاً دخولك كمسئول انقر **Continue** "متابعة"، وإلا أدخل حساب أحد المسئولين ثم انقر **OK** "موافق" سيظهر المربع الحواري **Properties** "متابعة" ويظهر فيه اسم كارت الشبكة المثبت علي جهازك في خانة **Connect Using** "الاتصال باستخدام" شكل ٩–١.



شكل ٩–١ مربع خصائص الشبكة المحلية

٥. تأكد أن الخيار **File and Printer Sharing For Microsoft Networks** مختاراً (محدداً). فأن لم يكن انقر المربع الذي أمامه لاختياره كما يظهر في الشكل.



سوف نعود لشرح مشاركة موارد الشبكة بالتفصيل في الفصل السادس عشر

وحدة الخدمة المخصصة

أن استخدام جهاز كمبيوتر مستقل كوحدة خدمة مستقلة يحقق الكثير من المزايا ويناسب الشبكات الكبيرة التي تتطلب أعمالها نوعاً من السرية وتداول كمية كبيرة من البيانات . عند إنشاء شبكة، يجب أن تعرف كيف تستخدم جهاز الكمبيوتر الذي سيعمل كوحدة خدمة (أو كجهاز خادم أو كملقم أو **Server**) رغم أنه في الإمكان عمل أي جهاز علي الشبكة التناظرية كوحدة خدمة ووحدة عمل معاً إلا أننا نفضل تخصيص جهاز مستقل ليعمل كوحدة خدمة حتي وان كانت الشبكة تناظرية.

لماذا نلجأ إلي وحدة خدمة مخصصة

الحقيقة أن استخدام جهاز كمبيوتر كوحدة خدمة ووحدة عمل يسبب بعض المشكلات. من هذه المشكلات أنك تتوقف عن العمل مؤقتاً في كل مرة يحاول فيها مستخدم آخر الوصول إلي بيانات علي القرص الصلب لجهازك. هذا من ناحية ومن ناحية أخري فإنك تفقد الخصوصية علي جهازك ولابد من الحذر من ترك أية بيانات علي القرص الصلب لا ترغب في اطلاع الآخرين عليها بالإضافة إلي ذلك ربما يقع مستخدمو الشبكة في بعض الأخطاء التي تسبب لك مشاكل خطيرة مثل أن يقوم أحدهم بحذف ملف مهم من علي القرص الصلب لجهازك بدون قصد أو قد ينتقل إليك فيروس من أحد الأجهزة الأخرى. أو أن يسرف أحدهم في وضع ملفات كبيرة أو غير مهمة علي القرص الصلب مما يسبب تقليل المساحة التي تحتاجها لنسخ ملفاتك.

مواصفات جهاز وحدة الخدمة

لتهيئة وحدة الخدمة بصورة سليمة نورد فيما يلي بعض التوجيهات التى تعينك على تجهيز وحدة تلبى متطلباتك .

- يجب أن يحتوى جهاز الخدمة على معالج قوى وذاكرة كبيرة . تتطور المعالجات والذاكرات بصورة مذهلة . ولذلك من الصعب تحديد حجم معين. فقد أشير عليك بمعالج تصل سرعه إلى ٣ جيجا بايت وذاكرة قدرها ١ جيجا بايت ، وعندما يصلك الكتاب تجد أن هذا القدر قد تجاوزه الزمن.
- استخدم قرص صلب ذو مساحة كبيرة لتكفى مساحة البرامج والملفات المشتركة والملفات الخاصة التي ستوضع عليه. يمكن شراء قرص صلب يقاس حجمه بالتيرابايت.
- لا يلزم إن تكون الشاشة كبيرة وذات مواصفات عالية يكفى استخدام شاشة عادية وكارت فيديو معقول.
- يفضل استخدام محركات أقراص SCSI بدلا من IDE لأن SCSI يحقق أداء اعلي لوحدات خدمة الشبكة.
- يجب شراء صندوق للجهاز (Case) يحتوى على مزود طاقة جيد وقوى. ويحتوى على مساحات كافية تسمح بإضافة أقراص صلبة إضافية في المستقبل.

الخدمات الشائعة لوحدة الخدمة المخصصة

فى الشبكات الصغيرة التى تستخدم وحدة خدمة واحدة، من الشائع أن توفر وحدة الخدمة خدمات متعددة مثل خدمات مشاركة الطابعة والملفات ومشاركة القرص الصلب والتطبيقات .....الخ. أما فى الشبكات الكبيرة فإنها تلجا غالبا إلى تخصيص وحدة خدمة لكل نوع من الخدمات. يعتمد عدد وحدات الخدمة على الشبكة الكبيرة التى تزيد عليها الاتصالات عدداً من وحدات الخدمة أكثر مما تتطلبه شبكة صغيرة قد تكون قادرة على أن تستمد كل الخدمات الخاصة بها من وحدة خدمة واحدة أو أثنيتين. فيما يلى نذكر أهم أنواع وحدات الخدمة المخصصة والخدمات التى توفرها.

خدمات وحدات الخدمة المخصصة

فى الشبكات الصغيرة تستخدم وحدة خدمة واحدة للقيام بخدمات الملفات والطابعات والاتصالات ....الخ، وفى الشبكات الكبيرة–تبعا لحجمها–يتم توفير كل خدمة بنوع

معين من وحدات الخدمة. وليس معنى هذا أن كل خدمة يجب توفيرها بخادم مستقل.
يعتبر عدد الخادمات التى توفر خدمة واحدة أو خدمتين على حجم الشبكة. كلما زاد حجم الشبكة كلما زاد عدد وحدات الخدمة التى تستخدمها. فيما يلى توضيح لوحدات الخدمة المختلفة وأنواع الخدمات التى تقدمها.

وحدة خدمة الملفات **File Server**: توضع عليها الملفات التى تتم مشاركتها بين عدد من المستخدمين. عادة توضع الملفات التى يتم مشاركتها فى مجلد عام، ويمكن أن يشمل هذا المجلد العام مجلدات خاصة لمستخدمين معينين. وجود الملفات المهمة فى مكان واحد، يسهل عملية نسخ الملفات الاحتياطية بصفة دورية.

وحدة خدمة الطابعة **File Server**: توضع على وحدة خدمة الطباعة الطابعة الخاصة بالشبكة. وتعتبر وحدة الخدمة هذه بمثابة قناة التحكم للطابعة. تتولى وحدة خدمة الطباعة كل مهام الطباعة التى يتم توجيهها إلى الطابعة فى طابور حسب دورها. بدون وحدة خدمة مخصصة للطباعة الذى يحصل أن مهام الطباعة توضع مؤقتا على جهاز الكمبيوتر قبل إرسالها إلى الطابعة. تخصيص وحدة خدمة للطابعة يوفر مساحة القرص الصلب الضرورية لذلك.

وحدة خدمة تطبيقات **Application Server**: توضع على وحدة خدمة التطبيقات التطبيقات المهمة والمشتركة مثل قواعد البيانات المتخصصة وبرامج الحسابات أيضا توضع عليها البرامج الإنتاجية مثل **Microsoft Office**.توضع كذلك على وحدة الخدمة فئة أخرى من البرامج يطلق عليها **Group ware** "البرامج الجماعية" وهى عبارة عن برامج تسمح للمستخدمين بالاتصال والمساهمة، مثل البريد الالكترونى وبرامج جدولة المواعيد والاجتماعات والتقويم ومنها على سبيل المثال **Microsoft Exchange**.

وحدة خدمة اتصالات **Communication Server**: تسمح هذه الوحدة بتشغيل برامج متخصصة تسمح للمستخدمين على الشبكة بالاتصال كما تسمح للمستخدمين على الشبكة بمشاركة المعلومات مثل البريد الالكترونى ومجموعات المناقشة.

وحدات خدمة أخرى: تستخدم مع الشبكات الكبيرة لخدمات معينه مثل وحدة خدمة لويب لإنشاء موقع ويب يمكن الوصول إليه داخليا من قبل الموظفين أو ملقم DHCPالذى يمكن أن يوفر عناوين IP لمحطات العمل ديناميكيا.

اعتبارات هامة

فيما يلي بعض الاعتبارات التي يجب أخذها في الحسبان عند استخدام وحدة خدمة مخصصة.

- عند تخصيص جهاز كمبيوتر مستقل كوحدة خدمة مع الشبكات التناظرية، يجب أن تقوم بإعداد خيارات تهيئة وحدة خدمة الشبكة بحيث تحقق وظائف وحدة الخدمة أما إذا كنت ستستخدم نفس الجهاز كوحدة خدمة ومحطة عمل (جهاز تابع) فلابد من بعض خيارات تهيئة وحدة خدمة الشبكة حتي توازن بين هذه الخيارات لتحصل علي أفضل أداء لوظائف وحدة الخدمة والجهاز التابع من نفس الجهاز .
- حاول أن تقلل عدد وحدات الخدمة المستخدمة في شبكتك قدر الإمكان . فكلما قل عدد الوحدات المستخدمة على الشبكة ، كلما قل الجهد المستنفذ فى إدارتها .

ترشيد استغلال مساحة القرص الصلب

من المعروف أن مساحة القرص الصلب يتم شغلها بالكامل مهما اتسعت ، ومن هنا يجب تنظيم القرص الصلب بصورة جيدة حتى تتجنب إضافة قرص جديد إلى وحدة الخدمة فى كل مرة تمتلئ فيها مساحة القرص الحالى بالكامل . يجب على كل مستخدم أن يدرك قيمة المساحة المتاحة على القرص الصلب ويحسن استغلالها

إن أفضل طريقة لتحديد مساحة القرص الصلب المطلوبة على الشبكة، هى تحديد الملفات التي ستوضع على هذه الوحدة. يجب أن تكون هذه المساحة كافية لتخزين برامج الشبكة نفسها بالإضافة إلى مساحة ملفات البيانات والتطبيقات المشتركة وملفات البيانات الخاصة. ضع في اعتبارك أن نظام تشغيل الشبكة يشغل كما كبيرا من مساحة القرص الصلب عندما تقرر تخزين الملفات والتطبيقات المشتركة .

قيود الإدخال والإخراج

يرد علي وحدة الخدمة بعض القيود المتعلقة بالإدخال والإخراج ، الأولي قيود علي سرعة بطاقة الشبكة، والثانية قيود علي الوقت الذي تستغرقه لقراءة محرك القرص الصلب للخادم والكتابة عليه .

سرعة بطاقة الشبكة: عادة لا تمثل السرعة أهمية كبيرة إلا إذا كانت الشبكة لم يتم تصميمها بطريقة جيدة، وعليها عدد كبير من المستخدمين. ويتم تحديد السرعة التي ترسل بها البطاقة البيانات بواسطة نوع الشبكة. فعلي سبيل المثال إذا كان تخطيط الشبكة الخاصة بك هو **100 Base-T Ethernet** يتم إرسال البيانات بسرعة ١٠٠ ميجابت في الثانية، إما إذا كان التخطيط هو **ATM** أو**1000Base –T**، فقد تتمكن من إرسال البيانات بسرعة ١٠٠٠ ميجابت في الثانية .

سرعة محرك الأقراص الصلبة عند شراء محرك قرص صلب لاستخدامه مع جهاز الخادم، فكر في عدد الدورات في الدقيقة "**RPM**" ووقت الوصول(يقاس بالملي ثانية)، من المناسب أن تشتري قرص ذو **RPM** (عدد دورات فى الدقيقة) ١٠٠٠٠ أو أكثر وأقل سرعة وصول للبيانات علي القرص .

مجموعات RAID

كلمة **RAID** اختصار للعبارة **"Redundant Array Of Inexpensive Disks** " ويمكن ترجمتها كما يلى "مصفوفات متكررة من الأقراص غير المكلفة " .

وتعتمد فكرة مجموعات **RAID** علي استخدام التكرار بصفة متكررة في الخادمات.كما تذكر من الفصل الثاني عن الحديث عن الأقراص الصلبة أننا قلنا أن **SCSI** تُمكِّن ما يصل إلى سبعة أجهزة من الاتصال بجهاز الكمبيوتر فى سلسلة واحدة. وهذا معناه أنك يمكنك استخدام بعض وحدات **SCSI** الخاصة لإعداد محركات أقراص صلبة متعددة على سلسة واحدة مقاومة جدا لفقد البيانات. يطلق على هذا الإعداد اسم **RAID**. ويطلق على وحدات تحكم **SCSI** الخاصة التى تعالج **RAID** اسم وحدات تحكم **RAID**.

وللتوضيح نقول أنها تعتمد علي ربط مجموعة من محركات أقراص (ثلاثة أو أكثر) في سلسلة واحدة والتعامل معها علي أنها محرك واحدة، حتى إذا فقدت البيانات الموجودة على محرك أقراص يمكن لبقية محركات الأقراص أن تعيد إنشاء البيانات الموجودة علي المحرك الذي تعطل. إذن الفائدة من مجموعات **RAID** أنها تجنبك توقف العمل بالشركة بأكملها في حالة حدوث مشكلة ما في القرص الصلب للجهاز للخادم. لأنك بإمكانك ربط محركى أقراص أو أكثر معا فى سلسلة حتى إذا فقدت محرك أقراص، يمكن أن تعيد محركات الأقراص المتبقية إنشاء البيانات الموجودة على محرك الأقراص المتعطل.

من هنا تتضح أهمية **RAID** كأحد نظم تخزين البيانات الفعالة عي القرص الصلب .

تتسم محركات الأقراص في بعض نظم **RAID** بأنها تبادلية، أي أنه يمكن إزالة أحد محركات الأقراص بينما يكون نظام **RAID** مستمر في العمل بدون أن يشعر مستخدمو الشبكة بذلك . يعمل نظام **RAID** علي إعادة إنشاء البيانات التي كانت موجودة علي محرك الأقراص الذي تمت إزالته من خلال البيانات الموجودة علي محركات الأقراص الأخرى بعد استبدال المحرك المعيب، ويعمل المحرك الجديد بشكل جيد.

مستويات RAID

تعمل **RAID** باستخدام مجموعة متنوعة من الطرق التى تتم الإشارة إليها باعتبارها مستويات تتراوح بين **0،5**. تحتاج للتعرف على المستويات **0،1،5** نظرا لاستخدامها بكثرة.

- المستوى **0** من **RAID**:

المستوى **0** من **RAID** عبارة عن محركات أقراص صلبة متصلة بجهاز كمبيوتر بدون تكرار. ولذلك يتم استخدامها لمحطات العمل فقط لأن الخادمات هي التي تحتاج إلى تكرار، وفى المقابل يتم استخدام مستويات **RAID** من **1**إلى **5** بصبغة شائعة للخادمات.

- المستوى **1** من **RAID**:

يعتمد على ازدواج الأقراص، حيث يتم توصيل محركى أقراص **SCSI**بنفس الحجم

ببطاقة وحدة تحكم **RAID**، إلا إن الكمبيوتر يراها على أنها محرك أقراص واحد. فمثلا إذا وصلت محركى أقراص سعة كل منها **250** جيجا بايت بجهاز الكمبيوتر، سوف يراهما الكمبيوتر **250** جيجا بايت فقط بدلا من **500** وذلك لأن وحدة تحكم **RAID** تقوم بكتابة كل البيانات بصورة مطابقة للقرصين. فإذا فشل محرك أقراص يمكن أن يستمر محرك الأقراص الآخر فى العمل دون أن يتأثر المستخدمون أو يعرفوا بتعطيل محرك القرص وعندما يقرا لجهاز من القرص، فإنه يقرأ من قرصين مرة واحدة.

- المستوى **5** من **RAID**:

فكرة المستوى **5** من **RAID** مشابهه لفكرة المستوى **1**إلا أنه يتطلب حد ادنى يبلغ ثلاثة أقراص متساوية السعة.

يزيد **RAID5** عن **RAID1** أنه يقوم بحفظ معلومات عن الملف يطلق عليها "بيانات التماثل" على الأقراص الثلاثة. فإذا فشل أحد محركات الأقراص فى مجموعة **RAID**، يمكن استخدام بيانات التماثل على المحركين الآخرين لإعادة إنشاء البيانات على محرك الأقراص الذى فشل.

طبعاً **RAID5** أسرع بكثير من **RAID1**، نظرا لأن فى أى وقت يطلب المستخدم ملفا من وحدة الخدمة، تقراه ثلاثة أقراص فى وقت واحد وهذه السرعة مطلوبة لدى المستخدمين.

المبادلة الفعالة

رغم أن نظام **RAID** يعد نظاماً جيداً إلا أنه لا يكمل موضوع التكرار. حيث أن القرص الذي يفشل أثناء العمل يجب إصلاحه . لكن في أحيان عديدة لا يسمح نظام العمل بتوقف الشبكة إلا من أجل الصيانة النادرة، كما هو الحال في نظام شبكة يعمل علي خط إنتاج أو نظم الإغاثة أو الصرافة وما شابه ذلك، وكثيراً ما يشعر مديرو الشبكات بالحرج عند فشل أحد محركات الأقراص ولتفادي هذه المشكلة يستخدم نظام بسمي المبادلة الفعالة. وهو نظام يسمح بإزالة محركات الأقراص الصلبة من وحدة الخدمة

وإعادة إدراجها أثناء تشغيل الجهاز.

يطلق علي محركات الأقراص **Hot-Swappable** (قابلة للمبادلة الفعالة). ويقصد بفعالة في نظام المبادلة الفعالة أن النظام يستمر في العمل أثناء استبدال القرص وتعد كلمة مبادلة كلمة واضحة فهي تعني إزالة قرص تالف وإدراج قرص عامل مكانه. والحاصل فعلاً أن العديد من وحدات تحكم **RAID** تعمل في وضع يتيح سحب محركات الأقراص من النظام واستبدالها أثناء تشغيل الكمبيوتر أو كما أطلقنا عليه قبل قليل (المبادلة الفعالة).

يتم استخدام المبادلة الفعالة بصورة شائعة علي نظم **RAID** ، وعندما يتم إزالة محرك أقراص واستبداله ، يمكن للعديد من وحدات تحكم **RAID** نسخ البيانات تلقائياً إلي محرك الأقراص الجديد. ولن يشعر المستخدمون إلا ببطء النظام بعض الشئ.

ملخص الفصل

الوظيفة الأساسية لوحدة الخدمة هي تقديم الخدمة التي تتطلبها الأجهزة أو الوحدات التابعة علي الشبكة. ويجب أن تلبي وحدة الخدمة حاجة المستخدمين في نقل البيانات بسرعة، والتأكد من أمان البيانات وتكاملها. يجب أن تكون وحدة الخدمة أكثر قوة من نظم سطح المكتب أي تشتمل علي معالج أقوي وذاكرة أكبر وقرص صلب ذو مساحة كبيرة لكي تستطيع مشاركة الملفات والطابعة مع باقي مستخدمي الشبكة يجب تمكين خاصية مشاركة الملفات والطابعة.

نلجأ إلي استخدام جهاز كمبيوتر كوحدة خدمة مخصصة في الشبكات الكبيرة وكلما زاد حجم الشبكة كلما زاد عدد وحدات الخدمة التي تستخدمها. تلجأ الشبكات الكبيرة لتوفير وحدة خدمة لكل نوع من الخدمات مثلاً وحدة خدمة مستقلة للملفات ووحدة خدمة مستقلة للطابعة .... الخ.

تجنبك مجموعات **RAID** توقف العمل بالشركة بأكملها في حالة حدوث مشكلة في القرص الصلب لوحدة الخدمة.

تدريبات

١. اختر الإجابة الصحيحة

المهمة الأساسية لوحدة الخدمة (Server) هي :

أ – يشارك موارده مع أجهزة الكمبيوتر الأخرى علي الشبكة.

ب – يجب أن يلبي حاجة المستخدمين في نقل البيانات بسرعة.

جـ – يتأكد من أمان البيانات وتكاملها.

د – تمرير البيانات إلي وحدات تابعة متعددة بكفاءة.

هـ – كل ما سبق.

و – لا شئ مما سبق

٢. اختر الإجابة الصحيحة

يستخدم جهاز كمبيوتر كوحدة خدمة مستقلة للأسباب الآتية:

أ- توفير تكلفة الشبكة وتقليل أجهزتها.

ب-تأمين البيانات وتداول كمية كبيرة منها.

ج- ليعمل كل مستفيد مستقلاً عن باقي الشبكة.

٣. أكمل العبارة التالية:

من أمثلة وحدة الخدمة المستقلة .... و .... و ....

٤. ضع علامة (✓) أمام الإجابة الصحيحة وعلامة (✗) أمام الإجابة الخاطئة

يتحكم في سرعة وحدة الخدمة

أ- مدير الشبكة المسئول عنها.

ب- الوقت الذي تستغرقه للقراءة من محرك الأقراص.

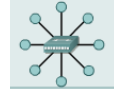
ج- سرعة بطاقة الشبكة.

٥. **الفائدة من استخدام مجموعات RAID أنها:**

أ- تعمل علي زيادة سرعة وحدة الخدمة وتأمين البيانات.

ب-تجنبك توقف العمل بالشركة بأكملها في حالة حدوث مشكلة في القرص الصلب لوحدة الخدمة.

ج- توفر لمدير الشبكة معلومات عن أجهزة الشبكة .





*في شبكة من نوع نظير/ نظير (**Peer-to Peer**) ، كل أنظمة التشغيل الصادرة بعد **Windows 3.11 for Workgroups** ابتداً من **Windows 95** حتي **Windows Server 2008** يمكنها تأمين الاتصال الشبكي. أما في حالة الشبكات من نوع الوحدة التابعة/وحدة الخدمة (**Client/Server**) فهناك أنظمة تشغيل تتناسب مع وحدات الخدمة وأنظمة تتناسب مع الوحدات التابعة.*

بانتهاء هذا الفصل ستتعرف على :

- *نظام تشغيل **Novell Netware**.*
- *نظام تشغيل **Microsoft Windows Server**.*
- *نظام تشغيل **UNIX***
- *نظم تشغيل **Mac OS X***
- *نظم تشغيل الشبكات النظيرة*

نقصد بنظم تشغيل الشبكات نظم التشغيل المصممة للعمل على الجهاز الخادم وهى غير أنظمة تشغيل سطح المكتب. والفرق بينهما أن نظام تشغيل سطح المكتب يصمم أساسا لتزويد المستخدم على محطة العمل الخاصة به بأفضل أداء للتطبيق الذي يستخدمه. أما نظام تشغيل الشبكة (خاص بالجهاز الخادم) فإنه يوازن بين احتياجات كل المستخدمين الذين يتصلون بالشبكة .

إذا كنت تنشئ شبكة لربط مجموعة كبيرة من الأجهزة وتقدم الكثير من الخدمات المركزية فلابد أنها ستكون من نوع الوحدة التابعة/وحدة الخدمة (**Client / Server**)

فيما يلى سنشرح باختصار أربعة من نظم تشغيل الشبكات:

- نظام تشغيل **Novell Netware**.
- نظام تشغيل **Microsoft Windows Server**.
- نظام تشغيل **Linux/UNIX**
- نظام **Mac OS X**

نظام تشغيل Novell Netware

يعد نظام التشغيل **Netware** من أقدم نظم تشغيل الشبكات وهو من إنتاج شركة **Novell** وصدر أول إصدار منه فى بداية الثمانينات (قبل ظهور نظام **Windows**) .

لأن نظام **Netware** تم تصميمه مبكرا، فلم تضع شركة **Novell** فى اعتبارها الانترنت.

ولذلك فإنها لم تنشئ دعما لبروتوكول**TCP/IP**وهو اللغة التى تستخدمها أجهزة الكمبيوتر للاتصال عبر الانترنت و لعل ذلك لأن هذا البروتوكول كان جديدا ولم يكن يعتمد عليه كما هو الحال اليوم .

لقد كان هذا النظام بمثابة وسيلة مريحة بالنسبة لمديري نظم ربط الشبكات الذين كانوا معتادين علي التعامل مع نظم الشبكات التي لا تعد ولا تحصي والتي ظهرت في الفترة من أوائل إلي منتصف الثمانينيات. لقد وفر **Netware** ربط شبكات بسيطاً ومؤمناً ويمكن الاعتماد عليه. وفي السنوات الأولي له حقق أرقاماً هائلة في المبيعات وتنافس عليه أصحاب الأعمال التجارية. بمرور السنوات تطور **Netware** وتجاوز استخدامه شبكة **LAN** المحلية

ليصل إلي توصيفات WAN ومع ظهور Netware 5 و Netware (NDS) Directory Service أصبح Netware منتجاً عالمياً.

إلا أن المفاجأة غير السارة حدثت عندما قدمت شركة Microsoft نظام التشغيل Windows NT في العام ١٩٩٤. وقامت بدعاية مكثفة له، مما أدي إلي تراجع مبيعات Netware وبالتالي تراجع حصة Novell في السوق بدرجة كبيرة. والخطأ الذي وقعت فيه شركة Novell أنها لم تنتبه إلي سرعة ازدهار وتطور الانترنت وانتشار الوعي العام بها، حيث استخدمت بروتوكول IPX الخاص بها لمدة تقرب من ١٥ سنة. وهو بروتوكول لم يضع في اعتباره الانترنت .

يستخدم نظام تشغيل الشبكة الجديد بروتوكول TCP/IP بصفته بروتوكول الشبكة الافتراضي للنظام . يوفر Netware 6 عدداً من الأدوات الجديدة وقد تم تصميمه للعمل فى الشبكات الأكبر من Netware 5.1 . رغم أنه بالإمكان استخدمه مع الشبكات الصغيرة. فيما يلى بعض الخصائص التى تميز نظام Netware 6.5:

- يستخدم نظاما متطورا لإدارة القرص الصلب يعرف باسم Novell Storage Services وهو نظام يتيح إدارة عدد هائل من الملفات من محرك أقراص واحد.
- الوصول إلى مجلدات وطابعات الشبكة من خلال اتصال قائم على الويب.
- تدعيم نظم الملفات فى نظم تشغيل الشبكات الأخرى(مثلWindowsوUNIXوLinux للوصول إلى البيانات على وحدة الخدمة من هذه النظم بدون الحاجة الى تثبيت برنامج خاص على الجهاز التابع.
- يوجد إصدار خارجى منNetware يعرف باسم Small Business وهو يشمل على إمكانيات إضافية تسهل التعامل مع الشبكة فى الشركات الصغيرة مثل برنامج البريد الالكتروني وجدولة مجموعة المستخدمين. يشتمل على مجموعة البرامج لتأمين الشبكة موجودة فى برنامج Border Manager.
- فى الإصدارات الأولى من Netware كانت الأدوات الإدارية ضعيفة، ولكن مع الإصدارات الأخيرة Netware 6.5 وجدت كثير من الأدوات الإدارية الجديدة. ومنها

مثلا برنامج **Netware Remote Manager**. يمكن استخدام هذا البرنامج لإدارة مساحات تخزين الشبكة ومراقبة إعدادات وحدة الخدمة. كما أن **Netware 6.5** أسهل فى الإعداد من الإصدارات السابقة

- قامت **Novell** بترقية تسلسل **Novell Directory Service** (خدمة دليل **Novell**) الهرمى لكائنات الشبكة إلى **Novell e Directory** (دليل **Novell** الالكتروني). وفر دليل **Novell** الالكتروني نظام تسلسل هرمى سهل الاستخدام لتعقب وحدات الخدمة، وغيرها من الكائنات على الشبكة.
- يمكن أن تمتد شبكة **Netware** لتشمل عدة شبكات **LAN** (يمكن استخدام شبكات **WAN**).

نظام التشغيل Microsoft Windows Server

في عام ١٩٩٢طرحت **Microsoft** نظام التشغيل **Windows NT Server 3.1** وتعني كلمة **NT**"**New Technology**" وكان هذا هو الإصدار الأول من نظم تشغيل الشبكات. وكان هذا هو النظام الذى طرحته ميكروسوفت لمنافسة كل من نظم **Netware** و **Unix** وحتى فى تلك الفترة لم يكن هناك فرق بين الإصدارات المنتجة من أجل وحدات الخدمة وتلك المنتجة من أجل الأجهزة التابعة (محطات العمل).

عندما أصدرت ميكروسوفت **Windows NT 3.5** كانت قد ابتكرت إصدارين مختلفين من نظم التشغيل. الأول للعمل على محطات العمل وكان اسمه **Windows NT Workstation** والثانى للعمل على وحدات الخدمة وكان اسمه **Windows NT Server**.

وجاء بعده **Microsoft NT Server 4.0** وقد حقق نجاحا ضخما، ولكنه لم يوفر أي نوع من التفرع الهرمي مثل ذلك الذي كان يوفره نظام **Netware** الذي أنتجته شركة **Novell**، لقد واجه هذا النظام بعض الصعوبات في الشبكات الكبيرة جدا، لأنه كان يعتمد علي نموذج النطاقات الذي يزودك بنوع من الحاويات التي تجمع فيها كل أجهزة كمبيوتر الشبكة والمستخدمين والموارد.

يمكن تعريف النطاق على أنه مجموعة من وحدات الخدمة (على الرغم من أن النطاق يحتاج إلى وحدة خدمة واحدة) وأجهزة الوحدات التابعة (محطات العمل) والمستخدمين وموارد الشبكة الأخرى التى تتم إدارتها بواسطة **Domain Controller** "وحدة تحكم فى النطاق".وتعد وحدة التحكم فى النطاق وحدة خدمة مسئولة عن تشغيل الشبكات وعن توثيق المستخدمين والموارد. مع وجود وحدة تحكم فى النطاق لكل نطاق كان مديرو والشبكات يواجهون بعض الأمور التى يجب معالجتها فى إدارة الشبكة، باستخدام بنية النطاقات هذه. وهذا ما تم معالجته فى الإصدار التالى وهو **Windows Server 2000**.

اشتملت برامج **Server** التى أنتجتها ميكروسوفت **(Windows Server 2000/2008)** على مجموعة ثرية من الأدوات والبرامج المساعدة التى كانت تنقص برامج **Workstation**. يستطيع **Windows XP** الاتصال بكل أنواع الشبكات ويتلاءم بصورة جيدة مع المؤسسات الصغيرة. أما **Windows Server 2003** فإنه كان يتعامل مع جزء وحدات الخدمات فى نظم الشبكات. ويعتبر نظاما مثاليا لوحدة خدمة الملفات والتطبيقات لأنه يستخدم واجهة **Windows** المألوفة للجميع.

نوضح فيما يلي باختصار الإصدارات الأخيرة من برامج تشغيل الشبكات التي أنتجتها شركة **Microsoft** في السنوات العشرة الأخيرة.

نظام التشغيل Windows Server 2000

وفر **Windows Server 2000** نوع من التسلسل الهرمي المنطقي لشبكات **Microsoft** عن طريق ما يسمي**Active Directory**أو"الدليل النشط"، حيث يسمح هذا الدليل النشط بإنشاء بنية منطقية تفرعيه للشبكة يمكن أن تحتوي علي أكثر من نطاق.

يوفر**Active Directory** (الدليل النشط)بنية تفرعيه تسمح لك بإنشاء بنية منطقية تفرعيه للشبكة يمكن أن تحتوى على نطاقات متعددة. من هذا تفهم أن النطاق مازال يعمل بصفته الوحدة الأساسية لبنية مايكروسوفت، وسوف يظل كل نطاق يدار بواسطة وحدة تحكم فى النطاق. تعد أكبر وحدة تالية فى بنية **Active Directory** هى التفرع. يتكون التفرع من نطاق جذرى. وهو النطاق الأول الذى تصفه على الشبكة. يمكن أن تحتوى

التفرعات على نطاقات متعددة. تعد النطاقات التى يتم إضافتها إلى التفرع نطاقات فرعية.عند إنشاء شبكة **Microsoft** سوف تحتاج إلى وضع وحدة تحكم فى النطاق عبر الشبكة وإنشاء النطاق لتفرع **Active Directory**.

هناك ثلاثة إصدارات من **Windows Server 2000**

Windows Server 2000 : وهو نظام التشغيل الرئيسي. صمم هذا الإصدار للاستخدام في الشبكات الصغيرة أو متوسطة الحجم، وهو يوفر جميع الإمكانيات الرئيسية لوحدة الخدمة مثل المشاركة في الملفات أو الطابعات، كما يعمل علي وحدة خدمة الانترنت ووحدة خدمة البريد الالكتروني.

Windows Server Advanced : يحتل المرتبة الثانية بعد **Windows Server 2000**. وقد تم تصميمه للعمل في الشبكات الكبيرة. ويدعم هذا النظام وحدات الخدمة ذات الذاكرة الكبيرة (**RAM**) الكبيرة بالإضافة إلي أربع وحدات معالجة متكاملة بدلاُ من المعالج الواحد الذي تقتصر عليه أغلب الأجهزة المكتبة ووحدات الخدمة.

Windows Server 2000 Data Center : يدعم هذا الإصدار وحدات خدمة تحتوي علي معالجات (**Processors**) وذاكرات كبيرة جداً وتم تصميمه خصيصاً لتطبيقات قواعد البيانات الكبري.

نظام التشغيل ***Windows Server 2003*** : يعد **Windows Server 2003** أسهل نظام تشغيل شبكات من حيث التثبيت والصيانة، كما أنه من السهل إدارته، ويوفر أمنا أفضل، بالإضافة إلى أنه يقدم دعما رائعاً للويب:

سوف تشعر مع **Windows Server 2003** بألفة لأنه يستخدم واجهة **Windows** الشهيرة.

وفيما يلى نتحدث بشيء من التفصيل عن **Windows Server 2003** باعتباره من أحدث نظام تشغيل أنتجته شركة ميكروسوفت.

مزايا Windows Server 2003

يشمل **Windows Server 2003** على الكثير من المزايا التى جعلته يتربع على عرش أنظمة تشغيل الشبكات فى هذه الأيام والتى تجعلك تفضله على كل من **Windows NT4** و **Windows Server 2003** . ياتى هذا النظام فى عدة إصدارات أقلها وحدة خدمة الويب وأعلاها وحدة خدمة مراكز البيانات المعقدة. تشمل كل إصدارات النظام على دعم داخلى لتقنيات "دوت نت" **NET**. التى تسمح بالاتصال بين الأفراد والنظم والأجهزة لتبادل المعلومات ومصادر الكمبيوتر باستخدام خدمات **XML(Extensible Mark up Language)** وتعنى "لغة الترميز القابلة للتوسعة". تتضح أهمية **Windows Server 2003** والتى تميزه عن الإصدارات السابقة فيما يلى:

- أسهل فى التثبيت حيث يشتمل على ميزات جديدة مثل ميزة التوصيل والتشغيل **(Plug and Play)** المحسنة، وقاعدة بيانات برامج التشغيل الموسعة والتحسينات العديدة التى تمت على برنامج الإعداد.
- يعد الدليل النشط **Active Directory** خطوة متقدمة على الدليل النشط فى **Windows Server 2000** ويضمن تحسينات على عضوية المجموعات والمزامنه وغيرها.
- أدت التحسينات التى أدخلت على برنامجى **Microsoft Management** تختصر: **(MMC)** و**IntelliMerror** واللذين يتيحان نقل إعدادات وملفات المستخدم من جهاز لآخر من خلال أى شبكة اتصال، إلى سهولة فى إدارة النظام بالإضافة إلى تحسينات فى أدارة الملفات.
- يقدم أمنا أفضل للشبكات من خلال معالجته للأخطاء فى مراقبة **IPsec** وتحسينات كثيرة فى إنشاء وإدارة نهج المجموعات.
- يقدم خدمات محسنة فى خدمة معلومات الانترنت **IIS** وميزات جديدة فى بروتوكول **DHCP**، ونظام اسم المجال **DNS**، وسطح المكتب البعيد، وإعادة توجيه الخدمات.
- بدمج تقنيات **NET**. التى أنتجتها مايكروسوفت والتى تقوم بتضمين وسائل لاستخدام

XML فى نظام التشغيل لربط التطبيقات والخدمات والأجهزة معاً فى حل واحد عبر الانترنت.

- **وأخيرا يمكننا أن Windows Server 2003 أسرع من وWindows NT4 أو Windows Server 2000**

إصدارات Windows Server 2003 المختلفة

يأتى Windows Server 2003 فى أربعة إصدارات يمكن شراء أى منها على حده

- **إصدار الويب Web Edition.لاستضافة مواقع الويب الصغيرة وتشغيل معلوماتIIS.**
- **الإصدار القياسى Standard Edition. للمؤسسات الصغيرة والمتوسطة .**
- **إصدار المؤسسات Enterprise Edition للمؤسسات الكبيرة.**
- **إصدار مركز البيانات Datacenter Editionللمؤسسات الكبيرة جداً وخاصة التى تعمل فى مجال مستودعات البيانات ومعالجة التجارة الالكترونية عبر الانترنت.**

نظام التشغيل Windows Server 2008

هذا هو الإصدار الأخير حتي لحظة إعداد هذا الكتاب وقد قدمت شركة ميكروسوفت في هذا الإصدار العديد من المزايا الجديدة من أهمها:

- **سهولة الاستخدام**
- **حماية الشبكات من الاختراق وزيادة عوامل الأمان والسرية.**
- **إمكانيات جديدة متكاملة لإدارته.**
- **إمكانيات التفاعل مع نظم تشغيل أخري مثل Linux و Unix .**

لقد أنفقت ميكروسوفت العديد من السنوات والكثير من المال لكي يخرج Windows server 2008 في صورة تلبي طموحات المستخدمين وتساعد في حل المشاكل التي واجهتهم في الماضي ولذلك فقد جاء Windows Server 2008 بالفعل في صورة متكاملة.

لقد بني Windows Server 2008 علي الإصدارات السابقة، ابتداءً من Windows 2000 ثم Windows Server 2003 ثم Windows Server 2003 R2 لكي يقدم

لمستخدمي النظام وظائف متكاملة لكل من الشبكات السلكية واللاسلكية مهما كان حجمها.

منذ أن بدأت ميكروسوفت في طرح نظام تشغيل شبكات **Windows NT**، فإنها تقدم كل إصدار في أكثر من طبعة **Edition** فمع **Windows Server 2003** مثلاً قدمت ٤ طبعات في البداية وهما **Standard Edition , Web Edition , Enterprise Edition , Data Center Edition**. ثم أضافت طبعات جديدة فيما بعد .

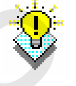
وقد اتبعت ميكروسوفت نفس الطريقة مع **Windows Server 2008**، فقد صدر **Windows Server 2008** في عدة طبعات هي :

- **Windows Server 2008 Standard Edition**
- **Windows Server 2008 Enterprise Edition**
- **Windows Server 2008 Data Center Edition**
- **Windows Server 2008 Web Edition**

وكلها تستخدم تقنية معالج **64 bit** وتقنية **32bit** السابقة. ومع ذلك توجد من الإصدارات الثلاثة الأولي وهي **Standard-Enterprise- Web** ، إصدار يعمل بتقنية معالج **32bit** فقط ويطلق عليه بالترتيب:

- **Windows Server 2008 Standard Edition without hyper-V**
- **Windows Server 2008 Enterprise Edition without hyper-V**
- **Windows Server 2008 Data Center Edition without hyper-V**

وقد أعلنت ميكروسوفت أن الإصدار الجديد من **Windows Server 2008** والمسمي **Release2** أو **R2** سيعمل فقط بتقنية معالج **64bit**. وأن تقنية **32bit** لن تعمل في المستقبل.



في هذا الفصل قدمنا فقط نظرة عامة على نظام تشغيل الشبكات **Windows** بإصداراته المختلفة مع التركيز على نظام **Windows Server 2003/2008**. لمزيد من التفاصيل عن تثبيت النظام وتوصيفه وتوصيف محطات العمل....راجع كتاب متخصص فى **Windows Server 2003/2008**.

نظام التشغيل UNIX

لقد كان نظام **UNIX** أحد نظم تشغيل ربط الشبكات الأولى، وفى البداية كان **UNIX** يعد نظام تشغيل لخبراء الكمبيوتر ولم يعترف به كنظام تشغيل شبكات وبالتالى لم يتم التعامل معه بصورة جيدة.رغم أن تكلفة كانت قليلة لأنه لم يستطع منافسة نظم التشغيل السائدة فى ذلك الوقت مثل **VM** من أنتاج **IBM** . تطور **UNIX** فى أشكال متعددة وتناوله أكثر من شركة حتى استقر على الإصدار الذى هو عليه الآن.

مع أن نظام **UNIX** من أكفأ نظم تشغيل الشبكات، إلا أن واجهة استخدامه صعبة. يعمل نظام **UNIX** علي وحدة الخدمة أو علي الوحدة التابعة (محطة عمل) ولكنه علي وحدة الخدمة أكثر قوة من محطة العمل.

يلائم **UNIX** مدير الشبكة المتمرس لأنه يمكن أن يحقق أي مهمة صعبة وبصورة يمكن الاعتماد عليها أما المستخدم العادي فإنه يجد فيه صعوبة .

مفاهيم UNIX الأساسية

- فى نظام **UNIX** يعد كل شيء ملفاً. بمعنى ليس فقط ملفات البرامج والبيانات تعتبر ملفات ولكن أيضا تعتبر محركات الأقراص الصلبة من وجهة نظر **UNIX** ملفا.
- يمكن **UNIX** نظم الملفات من استخدام مساحة القرص المتوفرة سواء أكان هناك قرص أو حتى ٥٠قرص فى النظام، هذا يجعل نظم الملفات قابلة للتوسيع بصورة كبيرة. نظرا لأنه يمكن مد أكثر من نظام ملفات واحد على أكثر من قرص، فإن مفهوم نظام الملفات يصبح مستقلا عن مفهوم القرص المادى.
- من الصعب تحديد تسلسل هرمى معين للأدلة بصفة التسلسل الهرمى المحدد لنظام **UNIX**.

نظام التشغيل LINUX

نظام تشغيل تم ابتكاره في أوائل التسعينات بواسطة شخص يدعي **LINUX** وأطلق عليه **LINUX** وهو يشبه نظام **UNIX**، هذا النظام مفتوح وتم وضعه علي الانترنت بحيث يستطيع أى مبرمج من المحترفين عمل تحسينات عليه، وبالطبع لابد أن تكون تكلفته بسيطة.

كلمة مفتوح تعني أنه بإمكانك الحصول علي النظام وعلي التعليمات المصدرية وعمل الإضافات والتحسينات التي تراها مناسبة لك.

يشتمل **LINUX** علي أدوات للاتصال بأي شئ تقريبا، ويمكن أن يستخدم **TCP/IP** كما يمكنه تشغيل بروتوكول **IPX.**

نظرا لأنه نظام مفتوح فيعتبر أكثر نظم تشغيل الشبكات شيوعا علي الانترنت. ولهذا السبب زاد عدد مستخدميه في السنوات الأخيرة.

نظام Macintosh OS X Server

نظم تشغيل الشبكات التي ذكرناها في الصفحات السابقة تعمل على أجهزة الكمبيوتر التي تستخدم معالجات شركة **Intel** أو معالجات متوافقة معها. ولذلك قامت شركة **Apple** بإصدار نظام تشغيل شبكات خاصة بأجهزة **Macintosh** يعرف باسم **Mac OS X Server** يحتوي هذا النظام على جميع الإمكانيات المتوفرة فى نظم تشغيل الشبكات المعروفة . مثل مشاركة الملفات والطابعة، وإمكانيات الاتصال بالانترنت ، وخدمات البريد الالكتروني ، وما إلى ذلك.

يتضمن **Mac OS X Server** الإمكانيات التالية:

- وحدة خدمة ويب تعمل ببرنامج **Apache**
- إمكانية لإدارة أجهزة الكمبيوتر التابعة على الشبكة تعرف باسم **NetBoot**
- خدمات ملفات من خلال بروتوكول **AFP**
- أداة **Web Objects** . وهي أداة لإنشاء مواقع الويب تعرف بجودة النتائج.
- برنامج **Quick Time Sharing Server** الذي يسمح لوحدة الخدمة ببث برامج متعددة الوسائط عبر الشبكة.

نظم تشغيل الشبكات النظيرة Pear to Pear

جميع نظم تشغيل الشبكات التي شرحناها حتى الآن ، تستخدم مع الشبكات من نوع Client/Server. إلا أن هناك أنواع أخري من نظم التشغيل تستخدم في الشبكات التي توفر خدمات نظيرة ومن أهمها نظام Microsoft Windows . فيما يلي سوف نوضح باختصار نظم تشغيل الوحدات التابعة التي توفر خدمات نظيرة وسوف نركز علي ربط الشبكات النظيرة باستخدام Microsoft Windows باعتباره نظام التشغيل الشائع المستخدم مع أجهزة الكمبيوتر المكتبية والذي نراه عادة على سطح المكتب.

في شبكة Pear to Pear Network "نظير بنظير" لا يوجد Network Operating System (اختصار NOS) (نظام تشغيل شبكة) وإنما يكون لمحطة عمل (وحدة تابعة) كل مستخدم برنامج نظام تشغيل سطح مكتب يمكنه مشاركة الموارد مع أجهزة كمبيوتر أخرى متى أراد . وتشتمل نظم التشغيل بداخلها على القدرة على توصيف بروتوكول ومشاركة الموارد . وعادة توفر نظم تشغيل الشبكات النظيرة عددا محددا من الأجهزة القابلة للمشاركة .

نظم تشغيل الوحدات التابعة (محطات العمل)

نظم التشغيل التي توفر خدمات نظيرة هي

- *نظام **Microsoft Windows*** : ابتدأ من نظام التشغيل Microsoft Windows for Workgroup 3.11 والإصدارات التالية له وفرت جميع نظم Windows إمكانات هائلة للشبكات النظيرة. فقد اشتمل Microsoft Windows XP (بإصداريه Home و Professional) علي ميزة Network Setup Wizard "معالج إعداد الشبكة" الذي يسهل من توصيف مجموعة عمل Windows ، حيث تعد مجموعات العمل شبكة نظيرة راجع ربط شبكات Windows النظيرة في Windows Vista في الفصل الرابع عشر من هذا الكتاب).

- ***نظام Linux*** : يوفر **Linux** عدداً من الطرق لمشاركة الملفات وغيرها من الموارد مثل الطابعات. ويوفر أيضاً ما يدعى (**NFS**) **Network File System** " نظام ملفات الشبكة" . حيث يمكن لجهاز كمبيوتر **Linux** العمل بصفته وحدة خدمة ووحدة تابعة في نفس الوقت . تتضمن معظم إصدارات **Linux** ما يسمي **Server Message Black** وتختصر هكذا **SAMBA** "كتلة رسائل الخادم" وتستخدم لتضمين أجهزة كمبيوتر **Linux**.
- ***نظام Macintosh OS X*** : لقد كان ربط الشبكات النظيرة جزءا من النظام **Mac OS** منذ البداية. وهو النظام الذي أصدرته شركة **Apple Macintosh**. وجدير بالذكر أن أجهزة كمبيوتر **Mac** لا تعتمد على **Intel** .

ملخص الفصل

شرحنا في هذا الفصل نظم التشغيل الموجودة في الأسواق، وبدأنا بنظام التشغيل **Netware** من إنتاج شركة **Novell** كواحد من أقدم نظم تشغيل لشبكات "الوحدة التابعة/وحدة الخدمة" **Client/Server**. وقد تطور في عدة إصدارات علي مر السنين إلا أن ظهور نظام تشغيل **Windows** من شركة **Microsoft** سحب البساط من تحته.

ثم تناولنا نظام تشغيل شبكات **Windows** بإصداراته المختلفة ابتداء من **Windows NT Server 3.1** وانتهاء بـ **Windows Server 2008**.

ثم تطرقنا إلي نظام تشغيل **Unix** كأحد نظم تشغيل الشبكات الأولي وأخيراً شرحنا نظام التشغيل **Linux** كنظام مفتوح ولذلك فتكلفته بسيطة ونظام تشغيل **OS X** من إنتاج شركة **Apple** الذي يحتوي علي جميع الإمكانيات المتوفرة في نظم التشغيل المعروفة.

تدريبات

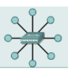
١. رتب نظم التشغيل الآتية من الأقدم إلي الأحدث.

أ. **Windows Sever 2003** ب. **Windows NT Server**

جـ . Windows Server 2000   د. Windows Server 2008

٢. صل العبارة الصحيحة والتي تحدد المعني الذي يخص كل نظام تشغيل.

نظام التشغيل	الوصف
١. نظام التشغيل Netware	أ – يعتبر تطويراً لنظام تشغيل Windows NT 3.5 ولكنه لم يوفر أي نوع من التفرع الهرمي الذي كان يوفره نظام Netware.
٢. نظام تشغيل Windows Server 2008	ب – نظام مفتوح تم وضعه علي الانترنت بحيث يستطيع أي مبرمج من المحترفين عمل تحسينات عليه.
٣. نظام التشغيل Linux	جـ – آخر إصدارات شركة Microsoft ويتميز بسهولة الاستخدام ويوفر للشبكة أماناً أكثر من الاختراق بالإضافة إلي إمكانيات متكاملة لإدارته وتفاعله مع نظم التشغيل الأخرى .
٤. نظام التشغيل Windows Server 2003	د – من إنتاج شركة Novell ويعتبر من أقدم إصدارات نظم تشغيل الشبكات وقد تطور في عدة إصدارات علي مر السنين.
٥. نظام التشغيل Windows NT Server 4.0	هـ – يتميز عن الإصدارات التي سبقته بسهولة التثبيت لأنه استخدم تقنية التوصيل والتشغيل (Plug and Play) ويتضمن تحسينات علي الدليل النشط. (Active Directory) علي الموجود في الإصدار Windows Server 2000



الباب الرابع

إنشاء الشبكات

الفصل الحادي عشر : التخطيط لبناء شبكة

الفصل الثاني عشر: تجميع الشبكة

الفصل الثالث عشر: اتصال الشبكة بالانترنت



يعد تخطيط شبكة جديدة وتنفيذها تحدياً بالنسبة لشخص متخصص في الشبكات. لابد أن يسبق بناء الشبكة تخطيطاً جيداً. لاشك أن إتباع أفضل الممارسات والتخطيط الجيد لبناء الشبكة، يساعد في بناء شبكة تناسب عملك لا تضطر لتغييرها أو لتحديثها قبل مدة معقولة .

بانتهاء هذا الفصل ستتعرف علي :

- *أفضل الممارسات*
- *الخطوات اللازمة للتخطيط الجيد لإنشاء شبكة اتصالات.*

قبل الشروع فى إنشاء شبكة يجب التخطيط جيدا لهذا الأمر. و لا يتطلب وضع خطة للشبكة أن تكون خبيرا بالكمبيوتر فيمكنك إنشاء شبكة بنفسك بإتباع التعليمات الواردة بهذا الكتاب. ولكن قبل شرح كيفية التخطيط لبناء شبكة نوجه انتباهك إلى ما يلى :

- لا تتعجل فى الانتهاء من مرحلة التخطيط. فكر جيدا و افحص البدائل المختلفة.
- اكتب خطوات إنشاء الشبكة.
- اعرض خطتك على شخص ذو خبرة عالية لتستفيد من ملاحظاته .

إتباع أفضل الممارسات

قبل أن نتكلم عن الخطوات التى يجب إتباعها عند التخطيط لبناء شبكة اتصالات، يجب أن تلتزم بمقياس قابل للتداول يلتزم بأفضل الممارسات المحددة. حتى تضع خطة جيدة لبناء الشبكة يجب أن تحدد مجموعة من المفاهيم نوضحها فيما يلى:

- *حجم الشبكة*: يجب أن تجلس مع الشخص المسئول عن المؤسسة حتى تتعرف على احتياجاته بالضبط لتحدد التخطيط المناسب وحلول إدارة الشبكة وحلول توزيع البرامج. مثلاً الشبكة التى تشتمل على ٥ محطات عمل يجب أن يكون تخطيطها بسيط، أما الشبكة التى تشتمل على ٥٠٠ محطة عمل فإنها تحتاج لبناء وتخطيط أكثر عمقاً.
- *التوقعات المستقبلية*: اسأل نفسك أو اسأل الشخص المسئول كم محطة عمل سوف تشتمل عليها الشبكة بعد عام من الآن. تساعدك درجة النمو فى تحديد الأجهزة والمكونات التى تحتاجها بصفة أولية. مثلاً شبكة بها ٥محطات عمل سوف يكون بها ١٠محطات بعد عام تتطلب أجهزة ومرونة أقل من شبكة بها ٥محطات عمل سوف يكون بها ٥٠ محطة بعد عام. لاشك أن الإجابة على هذا السؤال سوف تفيدك فى الإجابة على النقطة الأولى.
- *ماهو نوع الخدمات المطلوبة*: يجب أن تعرف بالضبط هل ستحتاج لتوفير خدمات مثل خدمة ملفات المستخدمين أو خدمة البريد الالكترونى للمستخدمين أو خدمة الويب للمستخدمين وهل ستحتاج لتوفير خدمات أخرى للمستخدمين؟ الإجابة بنعم على أى

من الأسئلة السابقة توجهك لما يجب عمله على النحو التالى:

أ- إذا كنت ستوفر خدمة ملفات المستخدمين. ضع فى حسابك أنك ستحتاج لوحدة خدمة مخصصة لخدمة الملفات، وفى هذه الحالة ستحتاج لوحدة خدمة كبيرة الحجم تشتمل على مساحة تخزين كبيرة تسمح بتخزين الملفات وإجراء عمليات النسخ الاحتياطى.

ب- إذا كنت ستوفر خدمة البريد الالكترونى عبر الانترنت، ستحتاج لتعيين وحدة خدمة مخصصة لهذه المهمة. ربما تحتاج لتسجيل نطاق على الانترنت والتعاقد مع مزود خدمة انترنت للتعامل مع البريد.

ج- إذا كنت تحتاج لخدمة الوصول إلى الانترنت للمستخدمين، سوف تحتاج لتعيين وحدة خدمة مخصصة وموجه ونظام تأمينى (يمكنك استخدام وحدة خدمة البريد الالكترونى لخدمة الوصول إلى الانترنت أيضا.

د- إذا كنت ستحتاج لتوفير خدمات أخرى مثل الوصول بعد. ستحتاج إلى أجهزة كمبيوتر تخصص لمهمة توفير الوصول عن بعد بالإضافة إلي توفير وصول عن بعد تتم إدارته مركزياً راجع الفصل الخامس عشر "الاتصال بالشبكات في **Windows Vista** " لمزيد من المعلومات عن الاتصال عن بعد .

- التامين: يعد تامين الشبكة عنصرا مهما عند إتباع أفضل الممارسات المطلوبة. إذ أن البيانات أهم ما تمتلكه المؤسسة. سوف تحتاج لأن تكون علي دراية بالتهديدات الواردة من الانترنت، واتخاذ إجراءات ضدها عن طريق توصيف البرامج الموجودة لإزالة النقاط غير المخصصة، وعن طريق إضافة برامج تراقب النقاط غير المحصنة المتبقية. يمكن أن تأتي الهجمات من أي مكان، ويمكنك توفير دفاع ضد الهجمات التي تعرفها. تسريب المعلومات المهمة إلى المنافسين عمدا أو بدون قصد، قد يسبب كارثة للشركة. أدى انتشار المخربين والهاكرز الذين يعيشون من أجل اختراق شبكات الكمبيوتر وتصميم برامج الفيروسات للعبث بالبريد الالكترونى أو تدمير البيانات إلى تطوير تقنيات التأمين بخطى سريعة لغلق الطريق على هؤلاء. (سوف تعود لشرح تأمين الشبكة وحماية البيانات

عليها في الباب الثامن من هذا الكتاب)

إن الإجابة التي تحصل عليها علي مثل هذه الأسئلة (وغيرها من الأسئلة التي قد تنشأ أثناء التفكير في احتمالات الشبكة) ، تعتبر مستنداً يحدد ما ستكون الشبكة قادرة علي فعله.

يشمل التخطيط لبناء شبكة كمبيوتر ما يلى :

١. تجميع معلومات عن أجهزة الكمبيوتر فى الشبكة.
٢. تحديد الغرض من إنشاء الشبكة.
٣. تحديد نوع الشبكة .
٤. اختيار تخطيط الشبكة .
٥. اختيار نظام تشغيل الشبكة.
٦. بناء الشبكة(شراء مكونات الشبكة).
٧. قابلية التشغيل في بيئات مختلفة
٨. كتابة وترتيب ما تعلمته.

تجميع معلومات عن أجهزة الكمبيوتر

إذا كانت أجهزة الكمبيوتر موجودة بالفعل ومطلوب منك إنشاء شبكة لربط الأجهزة الموجودة فيجب أن تتوفر لديك المعلومات التالية عن جميع أجهزة الكمبيوتر :

- نوع المعالج وسرعته.
- سعة القرص وترتيب أجزائه.
- مساحة الذاكرة.
- إصدار نظام التشغيل المستخدم.
- نوع الطابعة المتصلة بجهاز الكمبيوتر .
- تعرف على البرامج المستخدمة على الجهاز.
- تعرف على الأجهزة الملحقة بالكمبيوتر مثل CD أوDVD أو محركات الأشرطة...وغيرها.

تحديد الغرض من إنشاء الشبكة

يجب أن تحقق الشبكة للمؤسسة أو الشركة التي تمتلكها أداء أفضل وأسرع وأكثر كفاءة. فإذا لم يتحقق ذلك فان الشبكة تصبح عديمة الجدوى.

يجب أن تجلس مع شخص مسئول بالمؤسسة لتتعرف منه على ما يمكن أن يجعل عمل المؤسسة أسهل ولابد أن تعرف منه السبب الذى من أجله ترغب المؤسسة فى استخدام الشبكة.

يجب أن تعرف حجم العمل التجاري وطبيعته. يساعدك هذا فى اختيار نوع الشبكة هل شبكة مركزية أو لا مركزية. تأكد من جميع الأسباب الداعية إلى إنشاء شبكة ثم تسجيلها. فيما يلى بعض الأسباب التي تكمن وراء إنشاء الشبكات

- تيسير عملية تبادل البيانات بين الموظفين بدلا من الاعتماد على الأقراص المغناطيسية في ذالك.
- المشاركة فى الموارد مثل الطابعة حتى يستطيع جميع مستخدمي الشبكة استخدام طابعة متصلة بأحد الأجهزة الموجودة على الشبكة بدلا من تخصيص طابعة لكل جهاز.
- توفير اتصال لجميع أجهزة الكمبيوتر بالانترنت
- إنشاء نظام بريد الكتروني لتسهيل توزيع التعليمات على الموظفين .
- زيادة سرعة العمل مع توفير الوقت

تحديد نوع الشبكة

يتم تحديد نوع الشبكة بناء علي حجم العمل وطبيعته. فالمؤسسات الصغيرة التي بها عدد قليل من الموظفين الذين يحتاجون إلى مشاركة البيانات وباقي المصادر(مثل الطابعة) لا تحتاج إلي شبكة تتطلب خادم مستقل ونظام تشغيل شبكة منفصل. استخدام شبكة من نوع نظير/نظير **Peer to Peer** في هذه الحالة يكون مناسباً أكثر لأنه يوفر كثيراً في تكاليف الشبكة. أما المؤسسات الكبيرة التي تستخدم عدداً كبيراً من المستخدمين فإنها لابد أن تستخدم الشبكات المركزية التي تستخدم خادماً أو خادمات لإدارة الشبكة. تسمي هذه الشبكة أيضا شبكة الوحدة التابعة/وحدة الخدمة "**Client/Server**" (راجع الفصل الرابع

لمزيد من المعلومات عن أنواع الشبكات)

اختيار تخطيط الشبكة

سواء اخترت شبكة صغيرة من نوع نظير إلي نظير أو شبكة مركزية من نوع وحدة تابعة/وحدة خدمة. يجب أن تحدد التخطيط الذي ستختاره للشبكة. في الشبكات النظيرة يمكن أن توصف شبكة نجميه بسيطة لتخفيض التكاليف. أما فيما يتعلق بالشبكات القائمة علي الخادمات فيمكن أن تستخدم شبكة ذات توصيف نجمي من نوع**100 Base–T**أو غيرها من شبكات **Ethernet** السريعة. تستخدم كل الشبكات الحديثة تقريباً بشبكة **Ethernet** تخطيط **100 Base–T** وتخطيط **Gigabit Ethernet** "ايثرنت السريع".

اختيار نظام تشغيل وحدة الخدمة.

هناك العديد من نظم تشغيل وحدة الخدمة تستطيع اختيار ما يناسبك منها ومنها :

نظام Windows Server 2003/2008

وهو أكثر نظم تشغيل الشبكات استخداماً وهو إصدار خاص من**Windows** بشكل جيد للعمل مع وحدة خدمة الشبكة ولأن هذا النظام أحد إصدارات**Windows** فإنه يتعامل مع البرامج مثل **Microsoft Office**. ننصح بشدة باختيار **Windows Server 2003** نظرا لانتشاره وسهولة تثبيته واستخدامه.

نظام Novell NetWare

وهو نظام قديم ويتطلب تخصيص جهاز واحد علي الأقل للعمل كوحدة خدمة علي الشبكة. ولأنه ليس احد إصدارات **Windows 2003/2008** فهو لا يمكنه تشغيل برامج **Windows**. عموماً تراجع استخدام هذا النظام بعد صدور **Windows Server**.

نظام Linux .

وهو نظام أقل تكلفة لأنه متاح لكل الناس. وهو نسخة من **Unix**. حصل **Linux** علي حقه من التطوير أكثر من غيره لأنه نظام مفتوح يستطيع أي فرد أو مجموعة تطويره.

بناء الشبكة (شراء مكونات الشبكة)

يعد تخطيط 100 Base–T من Ethernet تخطيطاً واسع الانتشار ومتعدد الاستخدامات. لذلك سوف نورد فيما يلي قائمة بالمكونات الضرورية لشبكة 100Base-T بفرض انك قررت بناء شبكة من هذا النوع.

- أجهزة كمبيوتر سواء كانت أجهزة محمولة أو أجهزة سطح مكتب.
- بطاقة شبكة 100Base–T. توضع واحدة علي كل جهاز.
- جهاز Hub أوSwitch به منافذ توصيل كافية لجميع محطات العمل.
- أسلاك توصيل كافية لتوصيل قاعدة توصيل RJ-45 بكل بطاقة شبكة بقاعدة توصيل RJ-45 لجهاز Hub أو Switch.

بالنسبة لتخطيط Ethernet 100Base-T تعد كابلات الفئة الخامسة Category 5 كافيه. أما تخطيط 1000Base-T أو Gigabit ربما تحتاج لكابلات Category 6 (الفئة السادسة).

قابلية التشغيل في بيئات مختلفة

يجب أن تضع في اعتبارك عند التخطيط لبناء شبكة، أن ربط الشبكات يتغير بسرعة هائلة. انظر إلي التغيير في مجال ربط الشبكات من سنة إلي التالية ومن شهر إلي الشهر التالي. خذ مثالاً علي ذلك شبكة الانترنت وما يطرأ عليها من تطور وراقب التنافس بين شركات نظم تشغيل الشبكات المختلفة. حيث تسعي كل شركة إلي السيطرة علي السوق.

انظر إلي النظم المفتوحة مثل Linux وما تجتذبه كل عام من مستخدمين جدد.

قد يصيبك هذا بنوع من الإحباط، إذ قد يتبادر إلي ذهنك السؤال التالي. كيف يمكنني مجاراة هذا المجال سريع التطور؟ لحسن الحظ الأمر ليس كذلك لأن الواقع أن هناك مقاييس لربط شبكات TCP/IP محددة تصنفها مجموعة يطلق عليها IETF، وتنشر تلك المقاييس في مستندات يطلق عليها RFCs وتعني Requests for comments "طلبات للتعليقات" تتوفر المقاييس المحددة في مستندات RFC للشركات المصنعة التي ترغب في استخدامها. وفي عالم البرامج وهندسة الشبكات يتم الالتزام بالمقاييس وتوفير منتجات

تناسب البرامج القديمة والجديدة . معني ذلك أنك يجب أن تكون علي دراية بمقاييس IETF و TCP/IP المختلفة . لست مطالباً بمعرفتها بالتفصيل ، ولكن علي الأقل يجب أن تعرف ماهية المقاييس وما هو التوحيد القياسي المعلق.

لاشك أن معرفتك بالمقاييس ستسمح لك بتجديد المنتجات التي تتوافق مع تلك المقاييس والتي توفر أفضل الإمكانات فيما يتعلق بقابلية التشغيل في بيئات مختلفة.

نتيجة لذلك، يجب أن تأخذ في حسبانك عند اتخاذ قرار اختيار الأجهزة والبرامج أن تكون متوافقة مع المقاييس.

كتابة وترتيب ما تعلمته

بعد الانتهاء من الخطوات السابقة. تأتى خطوة كتابة مستند يشتمل على مواصفات الشبكة ليتمكن منشئ الشبكة أو من يأتى بعده من فهم الشبكة لأن لديهم دليل مرجعي للتصميم الأساسى للشبكة. ويجب أن يشتمل التوثيق للمستند الذي يحوى المواصفات على ما يلى :–

- الغرض من الشبكة.
- استخدامات الشبكة .
- عدد الأجهزة التي ستشتمل عليها الشبكة.
- نوع الشبكة. هل شبكة نظيرة أم شبكة وحدة تابعة / وحدة خدمة.
- بناء الشبكة (مثلا Ethernet).
- التطبيقات التي ستوضع على كل جهاز.
- التعريفات المخصصة للمستخدمين وكلمات المرور لكل منهم.

ملخص الفصل

إن التخطيط الجيد يؤدي إلي بناء شبكة قوية ودائمة. وقد تعرضنا في هذا الفصل لشرح أفضل الممارسات التي تؤدي إلي وضع خطة جيدة لبناء الشبكة ثم شرحنا المعايير التي يجب الالتزام بها عند التخطيط لبناء شبكة كمبيوتر.

تدريبات

١. اذكر ثلاثة من الأمور التي يجب أن تكون علي دراية بها عند التخطيط لبناء شبكة كمبيوتر .

٢. من العوامل التي تحدد هل تختار شبكة مركزية أو لامركزية.

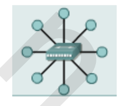
أ. حجم العمل التجاري وطبيعته.

ب. عدد الموظفين الذين يحتاجون لمشاركة البيانات وباقي المصادر .

ج. قابلية الشبكة للعمل في بيئات مختلفة.

د. كل ما سبق.

ه. لا شئ مما سبق.





الفصل الثاني عشر
تجميع الشبكة

شرحنا فى الفصول السابقة المفاهيم الأساسية لتشبيك الكمبيوترات والأجهزة والبرامج التي تستخدمها لبناء شبكة وأخيرا تعرضنا لمعلومات مهمة عن كيفية التخطيط لبناء شبكة قبل الشروع فى توصيل أجزاء الشبكة معا. وبانتهاء هذا الفصل سوف تكون تعرفت على:

- *احتياطات الأمان.*
- *ماقبل التركيب.*
- *تركيب بطاقة الشبكة.*
- *توصيل الأسلاك .*
- *تثبيت نظام تشغيل وحدة الخدمة.*
- *تهيئة أجهزة كمبيوتر الشبكة.*
- *اختبار صحة تثبيت الشبكة.*

فى هذا الفصل ستعرف كيف تقوم بتوصيل أجهزة الشبكة بعبارة أخرى كيف تقوم بتثبيت أجزاء الشبكة التى شرحناها من قبل. قبل أن تقوم بتوصيل الشبكة، يتعين عليك اتخاذ مجموعة من احتياطات الأمان نوضحها فيما يلي.

احتياطات الأمان

نوجز فيما يلي بعض الاحتياطات التى يتعين عليك اتخاذها تجنبا للوقوع فى بعض المشاكل مثل تعرض أحد مكونات الشبكة للتلف أو تعرضك لمخاطر نتيجة لصدمة كهربية قد تقع لاقدر الله نتيجة لتوصيلات خاطئة .

على الرغم من أن المكونات المادية للكمبيوتر قد تبدو قوية وغير قابلة للتلف، فإنها ليست كذلك. يمكن لإلكترونيات الكمبيوتر والشبكة التي تعمل بالكهرباء أن تتلف أيضاً.

- قم بإغلاق **Windows** ثم اطفىء الكمبيوتر قبل عمل أى توصيلات أو تثبيت أحد مكونات الشبكة مثل بطاقة الشبكة أو غيرها ثم افصل الكهرباء عن الجهاز. وهذا الإجراء يجنبك تلف بعض مكونات الكمبيوتر كما أنه يضمن سلامتك من حدوث صدمة كهربية .
- استخدام الأدوات المناسبة. قد ترغب في استخدام أية أداة قديمة للعمل على أجهزة الكمبيوتر، لأنها لا تبدو ميكانيكية مثل السيارة –على سبيل المثال. على الرغم من ذلك، تأكد من أن الأدوات التي تستخدمها مناسبة. استخدم مفك **Philips** جيداً ومجموعة مفكات صمولة، إذا أمكن. يمكن الاستفادة من ملقاط صغير لالتقاط الأجزاء الصغيرة. يمكن الاستفادة أيضاً من كماشة. إذا كانت أي من الأدوات ممغنطة، عليك بإلغاء مغناطيسيتها (يمكن استخدام الحرارة) أو استبدلها – لا تتفق المغناطيسية وأجهزة الكمبيوتر معاً .
- افتح صندوق الكمبيوتر(**Case**) برفق حتى لا تتلف الالكترونيات الموجودة بداخل الصندوق والتي تستخدم فى تشغيل الكمبيوتر .

إذا كنت تفتح الصندوق ولم تتم إزالة الجزء العلوي بسهولة، لا تستخدم القوة معه. يمكن أن يؤدي استخدام القوة في فتح صناديق الكمبيوتر إلى إتلاف الصندوق

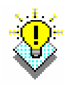
والإلكترونيات الدقيقة التي تجعل الجهاز مفيداً.

- تعرف جيدا على الكابلات والوصلات التى تقوم بفكها ويفضل أن تضع عليها علامات لتميزها ليسهل عليك إعادة تجميع الكمبيوتر بعد فكه .
- ضع علامات على كل الكبلات والوصلات إذا كان يجب عليك إلغاء توصيل أي شيء. يؤدي ذلك إلى تبسيط إعادة تجميع جهاز كمبيوتر تم فكه. يمكنك استخدام ، قلم تمييز لعنونة الكبلات، كما يمكنك أيضاً رسم بعض المخططات التي توضح أي كبلات تتصل بأية أجهزة. تعد أفضل طريقة لوضع علامات على الوصلات هي تلك التي تساعدك على إعادة توصيل ما تم فك توصيله. يمكنك استخدام شريط لاصق وقلم تمييز.
- تأكد من تركيب البطاقات فى الفتحات المناسبة لها . فمثلا لا تضع بطاقة **PCI** فى فتحة **ISA** أو العكس لأن ذلك إن حدث يؤدى إلى إتلاف البطاقة وربما جهاز الكمبيوتر. يمكن التمييز بين **ISA** و **PCI** بالحجم، حيث أن **PCI Slots** أصغر من **ISA Slots**
- إذا لم تطاوعك بطاقة الشبكة أثناء التركيب لا تتعامل معها بعنف.لأن القوة تؤدى إلى إتلافها .فى هذه الحالة ننصحك بسحب البطاقة والنظر إليها لتتعرف على سبب عدم ملاءمة البطاقة فربما تكون واجهة الفتحة غير صحيحة . أو أن الشريط المعدني في مؤخرة البطاقة (غطاء الفتحة) يعوق الطريق بطريقة ما.

لن يكون العمل على أجهزة ومكونات ربط الشبكات عملية صعبة إذا توخيت الحذر، إنه يتعلق فقط باحترام الخصائص المادية للكائن واستيعاب قدر القوة الكافي. لا تستخدم القوة مع أى شيء، إن لم يكن لديك اختيار.

تركيب بطاقة الشبكة Installing NIC

بعد الانتهاء من تثبيت الكابلات، يجب أن تبدأ فى توصيل الأجهزة بالشبكة وتهيئتها بحيث تعمل الشبكة بشكل جيد. نود التنبيه إلى أن معظم اللوحات الأم تأتى وعليها بطاقة شبكة. ولن تحتاج إلي الخطوات الآتية لتثبيت بطاقة الشبكة. ولكننا أوردناها هنا لأنك قد تصادف جهازاً يحتاج لتركيب بطاقة شبكة.



تذكر أن خطوات تثبيت بطاقة الشبكة الواردة فيما بعد ليست عامة، لأن أجهزة الكمبيوتر تختلف بصورة كبيرة. أن الهدف هنا هو استيعاب هذه الخطوات، وتعديلها لتتلاءم مع ما تجده عندما تفتح جهازك.

١. أطفئ جهاز الكمبيوتر وافصل مصدر الطاقة.
٢. افتح صندوق الكمبيوتر(Case)عن طريق فك المسامير الخلفية أو ضغط الصندوق (تختلف صناديق الكمبيوتر ولذلك عليك أن تراعي النوعية التي بين يديك هل يتم فتحها عن طريق تلك المسامير أم عن طريق ضغط الصندوق أو سحب أحد جوانبه). (راجع كتابا "تيسير صيانة وتجميع الحاسب")
٣. حدد الفتحة (Slot) التي ترغب في تركيب البطاقة فيها. يحتوي صندوق جهاز الكمبيوتر (Case)علي عدد الفتحات التي تسمي **Slots** مثل (**PCI Slots** و **ISA Slots** و **EISA**)
٤. عندما تجد الفتحة (Slot) المناسبة أزل الجزء المعدني الذي يحميها من خلف شاسيه الجهاز. إذا كان هناك مسمار يثبت به الجزء المعدني، قم بفكه واحتفظ به في موضع آمن . اجذب الجزء المعدني للخارج
٥. ركب البطاقة في الفتحة (Slot) مراعياً الآتي :

أ – اجعل البطاقة في محاذاة الفتحة وتأكد من أن جزء الورق المعدني الذي يشبه غطاء الفتحة يواجه الجزء الخارجي للكمبيوتر

ب – بمجرد أن تتم محاذاة البطاقة في الفتحة اضغط عليها برفق ولكن بثبات في الفتحة (قد تضطر لتحريك البطاقة للأمام أو للخلف)

جـــ– لا تستخدم القوة لإدخال بطاقات الشبكة في الفتحات. من المؤكد أن تؤدى هذه طريقة إلى إتلاف البطاقة وإبطال الضمان. إن لم تتلاءم البطاقة في الفتحة، اسحبها وانظر إليها. هل واجهة الفتحة الصحيحة؟ هل الشريط المعدني في مؤخرة البطاقة (غطاء الفتحة) يعوق الطريق بطريقة ما؟ غالباً ما يمكنك الفحص عن قرب

من اكتشاف سبب عدم ملاءمة البطاقة . وأحياناً يكون من الضروري ثني الجزء السفلي من الشريط المعدني لكي يتلاءم مع الفتحة – وفي أوقات أخرى، يجب تحريك البطاقة ببطء ورفق. يمكن أن تكون هذه العملية مرهقةً، ولكنها تمنع انشقاق اللوحات الأم. مما يتسبب في فشل الأجهزة والمكونات أكثر من أية كهرباء أستاتيكية في العالم.

٦. ثبت كارت الشبكة بالمسمار الذي أزلته في الخطوة الرابعة

٧. أعد تركيب غطاء صندوق الجهاز ثم وصل سلك الكهرباء واعد تشغيل الكمبيوتر.

في حالة بطاقات **NIC** التي تتسم بميزة **Plug and Play** "توصيل و تشغيل" سوف يتعرف نظام التشغيل علي البطاقة عند بدء التشغيل، ويصحبك خلال اختيار أفضل برنامج تشغيل للبطاقة.

مما سبق يتضح أن عملية تركيب البطاقات عملية سهلة. لكي تتم العملية بصورة صحيحة من أول مرة، ابدأ بالاطلاع علي كتيب الشركة المنتجة ثم حدد أية منتجات لها نفس واجهة البطاقة التي ترغب في تركيبها. إذا كان جهاز الكمبيوتر يحتوي علي أكثر من فتحة بواجهة تطابق واجهة بطاقة الشبكة ، استخدم الفتحة المفتوحة فليس هناك تفضيل بين الفتحات.

إعداد بطاقة الشبكة

إذا كنت تستخدم نظام تشغيل الشبكة **Windows Server 2003/2008** فإن إعداد البطاقة يتم تلقائيا باستخدام تقنية**Plug and Plug** (التوصيل والتشغيل) التى تحتوى عليها جميع نظم **Windows**الحديثة. إذا كان جهاز الكمبيوتر يحتوى بالفعل على بطاقة الشبكة، فسيقوم برنامج الإعداد بتثبيت هذه البطاقة بدون أخطاء. لكن إذا حدثت مشكلة ماذا تفعل؟ هنا يجب عليك قراءة الجزء التالى عن إعداد بطاقة الشبكة.

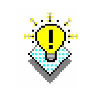
بافتراض أن بطاقة الشبكة تم توصيلها بطريقة صحيحة ولكنها مازالت لا تعمل. يمكن أن يكون أحد الأسباب الآتية هو السبب فى عدم عملها.

- إما أن برنامج تشغيل بطاقة الشبكة **(NIC Driver)** غير موجود أو مثبت بصورة غير صحيحة.
- الموارد المطلوبة غير متاحة.
- العيب فى البطاقة نفسها ولذلك فهى لا تعمل بصورة صحيحة.

وفيما يلي نوضح ذلك:

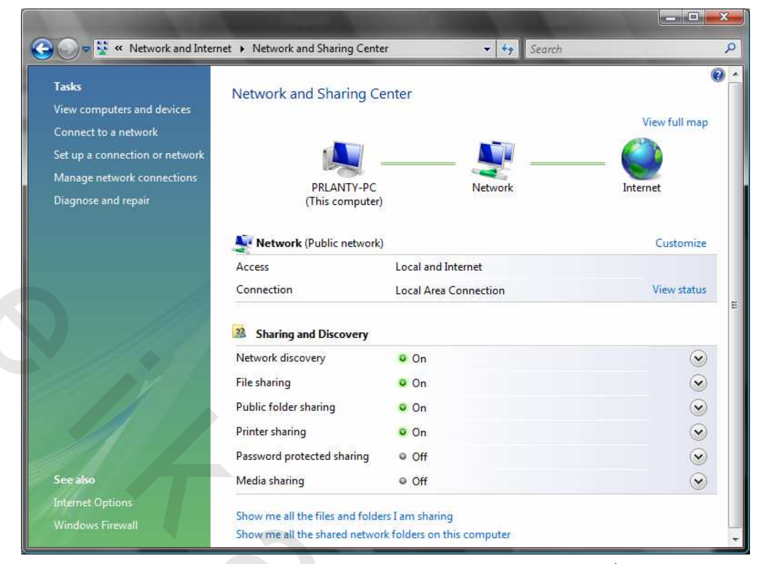
فحص برنامج تشغيل بطاقة الشبكة

أذا لم يكن برنامج تشغيل بطاقة الشبكة مثبتا. قم بتثبيته، أما إذا أردت فحص ما إذا كان هناك برنامج تشغيل مثبت أم لا فيجب عليك إتباع الخطوات الآتية:

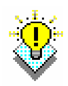


تم تجربة الخطوات الآتية على واجهة استخدام **Windows Server2003**. إذا كنت تستخدم إصدارات آخري فربما تواجه اختلافاً فى الخطوات.

١. افتح قائمة **Start** ثم اختر **Control Panel** ثم انقر **Network and Internet** ومن النافذة التي ستظهر اختر **Network and Sharing Center** تحصل على نافذة **Network and Sharing Center** . إذا ظهر بين خيارات القائمة الخيار **Local Area Connection** فهذا معناه أن برنامج تشغيل الشبكة مثبت بصورة صحيحة. وفى هذا الحالة لا داعى لمتابعة الخطوات التالية. وإلا فيجب عليك متابعة الخطوات معى. (انظر شكل ١٢–١)



شكل ١٢–١ نافذة **Network and Sharing Center**



ابتداء من هذه الخطوة ربما تحتاج لبرنامج تشغيل **Windows Server 2003** من أجل بطاقة الشبكة. تأكد أن برنامج تشغيل الشبكة بحوزتك أو قم بتنزيله من موقع الشركة المنتجة لبطاقة الشبكة. (ربما تحتاج للرجوع لفاتورة الشراء لمعرفة ماهية البطاقة، لأن هذه المعلومة لا يتم كتابتها على البطاقة). يجب عليك أولا تثبيت بطاقة وبرنامج التشغيل الخاص بها باستخدام **Add Hardware** في **Control Panel**.

٢. افتح قائمة **Start** ثم اختر **Control Panel** ثم **Add Hardware**. يتم فتح مربع **Add Hardware Wizard**.

٣. انقر **Next**. عندما تحصل على سؤال عما إذا كان الجهاز متصلاً أم لا، انقر **Yes** ثم انقر **Next** مرة أخرى. ستظهر قائمة بالأجهزة المثبتة تحت عنوان **Installed Hardware** إذا ظهر اسم بطاقة الشبكة ضمن القائمة ولم يكن بجوارها علامة تعجب (علامة التعجب تعني أن بطاقة الشبكة بها مشكلة). فهذا معناه أن البطاقة مثبته وتعمل بصورة صحيحة. وعليك إغلاق معالج إضافة الأجهزة بالنقر فوق زر **Finish**. وهنا

تتأكد أن المشكلة تتعلق ببرنامج تشغيل الشبكة وليس الشبكة نفسها.

٤. إذا لم تر بطاقة الشبكة ضمن قائمة **Installed Hardware**، انقر نقرا مزدوجا فوق **Add anew Hardware Device** فى نهاية القائمة. اختر **Install The Hardware That I manually Select From a List** ثم انقر **Next**.

إذا رأيت بطاقة الشبكة والى جانبها رمز مشكلة (علامة تعجب). انقر نقرا مزدوجاً فوقها، تحصل على رسالة **Device Status** تخبرك أن برنامج تشغيل الشبكة لم يتم تثبيته. انقر **Finish** لإغلاق **Add Hardware Wizard** وبدء أداة استكشاف الأخطاء وإصلاحها. سيتم فتح **Upgrade Device Driver Wizard**. انقر **Next**. ثم اختر **Display a List Known Drivers** ثم انقر **Next**.

فحص موارد بطاقة الشبكة

تتطلب معظم البطاقات أو الموائمات فى أى جهاز كمبيوتر موارد مخصصة لكى تعمل، تشتمل الموارد على شيئين منافذ**(I/O) Input/Output** وتعنى "الإدخال والإخراج" و**(IRQs) Interrupt Request** وتعنى "طلبات مقاطعة". ومن الأمور الثابتة، أنه لا يمكن لجهازين من أجهزة الكمبيوتر (نقصد بالجهازين مكونين من مكونات جهاز الكمبيوتر) مشاركة نفس الموارد. باستثناء أن أجهزة **PCI** يمكنها مشاركة **IRQs** "خطوط طلبات المقاطعة". فإذا حدث وتم تعيين نفس المورد لجهازين فسيحدث تعارض، ولن يعمل أحدهما أو كليهما بصورة صحيحة. سيتسبب ذلك فى عدم عمل بطاقة الشبكة وعدم ظهور رمز **Local Area Connection** فى نافذة **Network Connection**. نظرا لأهمية كل من الإدخال والإخراج **(I/O)** وطلب المقاطعة **(IRQ)** واحتمال أن تتعرض لأى منها لحل مشكلة بطاقة الشبكة سنتوقف قليلاً لشرح كل منهما.

فهم عناوين الإدخال والإخراج (I/O) وطلبات المقاطعة (IRQs)

نود فى البداية أن نطمئنك إلى أنك قد لا تضطر لتعيين إعدادات **I/O** أو **IRQ** يدويا، نظرا لأن بطاقات التوسعة فى الوقت الحالى أصبحت تعمل بمفهوم **Plug and Plug** (التوصيل والتشغيل) أى أن نظام التشغيل يقوم بتوصيفها تلقائيا ليتعرف عليها الكمبيوتر. لكن

الأمور لا تسير دائماً على ما يرام وقد تضطر لمعالجة مشكلة ببطاقة بها عيب أو معالجة جهاز قديم، فى هذه الحالة أفضل أن تفهم أساسيات هذه الاعدادت.

تستخدم معظم بطاقات الشبكة عناوين خارج قائمة العناوين شائعة الاستخدام. يعرض الجدول التالي قائمة بعناوين I/O الشائعة .

الجهاز	عنوان الذاكرة
COM1 (المنفذ المتسلسل رقم ١)	**03E8**
COM2 (المنفذ المتسلسل رقم ٢)	**02E8**
LPT1 (منفذ الطابعة)	**0378**
IDE Hard disk Controllers (وحدات تحكم IDE فى محرك القرص الصلب	**170** أو **1F0**
بطاقات الصوت	**220** و **330**

عناوين I/O شائعة الاستخدام

ولكن من أين تأتى المشكلة. افرض أن بطاقة شبكة تستخدم عنوان بالذاكرة هو 0360. بالنظر إلى جدول العناوين نجد أن هذا العنوان (وهو0360) لا يتعارض مع أى شيء. والمشكلة تحدث إذا استهلك برنامج تشغيل الجهاز مساحة كبيرة جداً. فإذا حدث ذلك فأنه سيشغل كل الطريق من 0360 إلى 0380 فى الذاكرة. مما يتعارض مع منفذ الطابعة وهو 0378.

عندما يضطر جهاز مثل بطاقة الشبكة أو بطاقة الفيديو إلى الحصول على انتباه الكمبيوتر بأكمله، فإنه يستخدم ما يطلق عليه IRQ. يعد IRQ أو Interrupt Request "طلب مقاطعة" هو طلب بأن يوقف النظام أى شيء آخر يؤديه فى تلك اللحظة. ويمنح انتباهه بالكامل للجهاز الذى يطلب الانتباه.

يعرض الجدول التالي إعدادات IRQ الشائعة

رقم IRQ	الوظيفة
٠	محجوز للاستخدام بواسطة نظام التشغيل (عداد وقت النظام)
١	محجوز للاستخدام بواسطة نظام التشغيل (وحدة التحكم في لوحة المفاتيح)
٢	يتم استخدامه للوصول إلى IRQ9 وما يليها. استخدمه فقط كحلٍ أخير.
٣	يتم استخدامه للمنفذ المتسلسل لاتصالات COM2 (غالباً ما يكون مضمناً في اللوحة الأم)
٤	يتم استخدامه للمنفذ المسلسل لاتصالات COM1 (غالباً ما يكون مضمنا في اللوحة الأم)
٥	عادة ما يكون غير مستخدم وغير متوفر.
٦	محجوز للاستخدام بواسطة نظام التشغيل (وحدة التحكم في محرك الأقراص المرنة).
٧	يتم استخدامه لمنفذ الطابعة (يطلق عليه أيضاً LPTI).
٨	محجوز للاستخدام بواسطة نظام التشغيل (ساعة النظام).
٩	عادة ما يكون متوفراً ، ولكنه كحلٍ أخير . ارجع إلى IRQ2 .
١٠	عادة ما يكون متوفراً.
١١	عادة ما يكون متوفراً.
١٢	يتم استخدامه غالباً من اجل أجهزة فأرة أداة النقل(على عكس أجهزة فأرة المنافذ المتسلسلة التي تتصل بمنافذCOM)
١٣	غالباً ما يكون غير مستخدم وغير متوفر.
١٤	يتم استخدامه عادة لوحدات التحكم في محرك أقراص Primary IDE (IDE الأساسي).
١٥	محجوز للاستخدام بواسطة وحدات تحكم IDE ثانوية.

إن ما يجب تذكره عند تركيب بطاقة شبكة هو محاولة عدم استخدام عنوان الذاكرة أو IRQ الذى تستخدمه البطاقات الأخرى أو اللوحة الأم. إذا فعلت ذلك، لن تعمل بطاقة الشبكة.

توصيل الأسلاك

بعد تركيب بطاقة الشبكة، فإن الخطوة التالية هي التعامل مع الأسلاك (إلا إذا كنت تعمل علي إعداد شبكة لاسلكية). يجب أن تضع جميع مستلزمات الشبكة (مثل الموجهات ورموز التبديل والموزعات) في مكان آمن، حتي لا يتمكن أي فرد من الوصول إلي أجهزة ومكونات الاتصال. فإذا لم يكن هناك احتمال لوجود نوايا سيئة ، فربما يؤدي الفضول البرئ إلي انهيار الشبكة. نتيجة لذلك يفضل إعداد خزانة للأسلاك.

تعتبر عملية توصيل الأسلاك مهمة شاقة. حيث يتم توصيل الأسلاك إلي أعلي أو أسفل أو عبر الأسقف وإلي أسفل الحوائط. ننصح أن تلجأ إلي متخصص بتوصيل أسلاك الشبكة. يؤدي ذلك إلي تقليل المشكلات بعض الشئ. وإذا حدث خطأ بالكابل فإن الشخص القائم بالتركيب سيمنحك ضماناً. لا تمرر كابلات الشبكة بالقرب من كابلات كهرباء التيار المار بالحائط بأقل من قدم واحد أي (٢٥سم) لأن دورة ٥٠ أو ٦٠ هرتز لكابل الطاقة يمكن أن تتداخل مع دورة إرسال البيانات.

يجب عليك توصيل سلك توصيل بين مقبس الشبكة 10/100 BASE-T الخاص بجهاز الكمبيوتر (يوجد علي بطاقة الشبكة التي ركبتها من قبل) ومخرج 10/100 BASE-T في الحائط. ثم تأكد من أن المنفذ المناظر علي لوحة التوصيل يتصل بالموزع (Hub) .

تثبيت نظام تشغيل وحدة الخدمة Server.

بعد الانتهاء من تثبيت الكابلات وكروت الشبكة لا يبقي سوي تثبيت نظام تشغيل الشبكة.

تختلف خطوات تثبيت نظم التشغيل باختلاف أنواع الشبكات (ننصح بالاستعانة بكتيب إرشادات نظام التشغيل لمزيد من التفاصيل)

فيما يلي بعض الاعتبارات التي يجب أخذها في الحسبان عند تثبيت نظام التشغيل علي وحدة الخدمة

تثبيت **Windows Server 2003**

تتم عملية تثبيت **Windows Server** بسهولة. ولكن قبل التثبيت يجب مراعاة الآتي:-

- كيفية تقسيم القرص الصلب الذي سيركب علي وحدة الخدمة. (هل القرص مقسم إلي أجزاء متعددة أم يستخدم كجزء واحد)
- نظام الملف المستخدم لكل مجلد. يدعم نظام **Windows 2000 /2003 Server** ثلاثة من نظم الملفات وهي : **Fat 32 – Fat – NTSF**
- اسم النطاق الذي تنتمي إليه وحدة الخدمة وهل تستخدم هذه الوحدة كجهاز تحكم في النطاق (النطاق هو مجموعة من أجهزة الكمبيوتر يتم إدارتها بصورة جماعية)
- اسم جهاز وحدة الخدمة .
- كلمة المرور

بعد تشغيل برنامج **Setup**. اتبع التعليمات التي تظهر لك علي الشاشة وقم بإدخال أي معلومات يطلبها البرنامج. يعرض البرنامج خيارات افتراضية تسمح لك بإنشاء وحدة خدمة عاملة.

تثبيت **Netware**

قلنا أن **NetWare** نظام قديم ولم يعد شائع الاستخدام، ولكننا نورد هنا من باب العلم بالشئ كيفية تثبيته . ويعد تثبيت **NetWare** أصعب من خطوات إعداد الشبكة .

استخدم القرص الذي يحتوي علي **Dos7** الذي يأتي مع **Netware** لتشغيل الجهاز وإنشاء **Dos** علي القرص الصلب لوحدة الخدمة . يمكن بعد ذلك تثبيت **NetWare** من **CD–Rom** الخاص بذلك .

بعد تشغيل برنامج التثبيت قم بإتباع التعليمات التي تظهر علي الشاشة لإتمام عملية التثبيت.

اختبار صحة تثبيت الشبكة

بعد الانتهاء من إعداد الشبكة، يجب اختبارها للتأكد أنها تعمل بشكل جيد. أبدا تشغيل وحدة الخدمة ثم الأجهزة التابعة لها وانتبه إلى أية رسائل خطأ قد تظهر عند تشغيل كل جهاز. سجل الدخول إلى الشبكة للتأكد من إمكانية الوصول إليها.

نورد فيما يلي بعض المعلومات التي قد تساعدك في التعامل مع بعض مشكلات الشبكة

إذا صادفتك مشكلة في الشبكة، فقم بفحص الكابلات وتحقق من أن جميع الروابط سليمة ومثبتة. تأكد من اتصال الأجهزة بالكابل بشكل صحيح.

- **للكشف عن سلامة كابلات UTP، انظر إلى اللمبة الموجودة خلف كارت الشبكة ووصلات جهاز HUB فإذا وجدت اللمبة تتوهج بصورة ثابتة فهذا يعنى أن الكابل سليم. أما إذا لم تكن اللمبة مضيئة أو كانت إضاءتها متقطعة، فعليك استبدال الكابل أو إعادة ربط الموصل.**
- **تأكد أن إعدادات كارت الشبكة صحيحة وذلك باختيارSystem من Control Panel ثم النقر فوق علامة تبويب Device Manger إذا لم يكن الكارت معداً بصورة صحيحة، تظهر علامة استفهام بجوار رمز كارت الشبكة.**
- **قم باستدعاء برنامج Network Control Panel وراجع جميع إعدادات الشبكة بدقة. تأكد من تنشيط البروتوكولات المطلوبة (NETBEUI أو IPX/SPX أو TCP/IP).**
- **إذا لم تعمل الشبكة بعد تطبيق الخطوات السابقة ننصح بتشغيل Networking Trouble Shooter في نظام Windows. ولتشغيل هذا البرنامج انقر فوق زر Start ثم اختر Help من القائمة التي تظهر وعندما يظهر مربع حوار Help انقر فوق Trouble Shooting. ثم اختر بعد ذلك الجزء الذي تريد تشغيله منه.**

ملخص الفصل

بدأنا في هذا الفصل بتوضيح احتياطات الأمان التي يجب أن تتبعها قبل الشروع في تجميع الشبكة. ثم شرحنا خطوات تجميع الشبكة فبدأنا بتركيب بطاقة الشبكة وإعدادها ثم شرحنا توصيل الأسلاك وأخيرا تثبيت نظام تشغيل وحدة الخدمة.

تدريبات

١. اذكر ثلاثة من احتياطات الأمان التي يتعين إتباعها قبل البدء في تجميع الشبكة

٢. اختر الإجابة الصحيحة

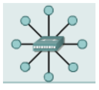
أ. يقوم مفهوم التوصيل والتشغيل (**Plug and Play**) بتوصيف إعدادات **I/O** تلقائياً عند تركيب الشبكة.

ب. تأتي معظم الأجهزة الحديثة مركباً بها بطاقة شبكة ولن تحتاج لتثبيتها يدوياً .

ج. يتسبب مشاركة نفس الموارد لأكثر من جهاز من أجهزة الكمبيوتر في حدوث تعارض بسبب توقف أحدهما أو كليهما عن العمل.

د. كل ما سبق.

ه. لا شئ مما سبق.





الفصل الثالث عشر
اتصال الشبكة بالانترنت

نشرح في هذا الفصل كيف تصل شبكتك بالانترنت لتستفيد من مزايا الاتصال بالانترنت مثل استخدام بريد الانترنت أو غيره من تطبيقات الشبكة.

بانتهاء هذا الفصل ستتعرف علي :

- *فكرة الانترنت*
- *الاتصال بالانترنت من خلال الهاتف (أجهزة المودم).*
- *الاتصال بالانترنت من خلال تقنية **DSL***
- *الاتصال بالانترنت من خلال تقنية **Cable Modem***
- *الاتصال بالانترنت من خلال تقنية **ISDN***
- *خطوط **T1** و **T3** السريعة*
- *خدمة الأقمار الصناعية*
- *الاتصال اللاسلكي*
- *المشاركة في اتصال الانترنت*

فكرة الانترنت

فى الحقيقة يصعب وضع تعريف جامع لمفهوم الإنترنت، وعموماً يمكن تعريفها بأنها مجموعة من أجهزة الكمبيوتر التى تتحاور مع بعضها البعض من خلال اتصالها عبر كوابل الخطوط التليفونية والألياف الضوئية والأقمار الصناعية وغيرها من وسائل الربط الشبكى.

عن طريق الانترنت يمكنك الاطلاع على جميع المعارف والمعلومات فى كافة المجالات وحقول المعرفة، فهى تضم آلاف المكتبات وقواعد البيانات، كما يمكنك من خلالها استخدام البريد الالكترونى، وتبادل البيانات مع الآخرين فى كل أنحاء العالم، والاشتراك فى المجموعات الإخبارية والرد عليها، والتسوق الالكترونى، والدعاية لمنتجاتك، والاطلاع على كل جديد فى كل نواحى الحياة المعاصرة.

تقنيات الاتصال بالانترنت

لكي تستفيد من الانترنت، يجب أن تتصل شركتك بالانترنت. هذا معناه أنك يجب أن تؤسس اتصالاً بشبكة الانترنت العالمية.

للاتصال بشبكة الانترنت يجب إن يتوفر لديك كمبيوتر وخط تليفونى بالإضافة إلى الحصول علي خدمة اتصال من مزود خدمة الانترنت ويطلق عليه **Internet Service Provider** وتختصر هكذا **ISP** . ويقدم مزود خدمة الانترنت هذه الخدمة مقابل اشتراك شهري .

يتم الاتصال بين الشبكة الداخلية وشبكة الانترنت بطرق عديدة. أهم هذه الطرق ما يلي:

- الاتصال من خلال الهاتف
- الاتصال من خلال **DSL** أو الكابلات
- الاتصال باستخدام تقنية **ISDN**
- خطوط الاتصال **T1** و**T 3** السريعة

وفيما يلي نلقي نظرة علي وسائل الاتصال هذه.

الاتصال من خلال الهاتف Dial-Up Connection

يعتمد الاتصال بالانترنت من خلال الهاتف علي استخدام مودم (Modem). وهو عبارة عن جهاز يسمح باتصال جهاز كمبيوتر بآخر عبر خط تليفون. عند الاتصال بالانترنت يستخدم المودم الخط التليفوني للاتصال بمزود خدمة الانترنت الذي قمت بإعداد حسابك معه. ولذلك فنحن نقول عن الاتصال عبر المودم "الاتصال الهاتفي" أو Dial-Up وفيها يتم الاتصال برقم يعطيه لك مزود الخدمة (ISP) Internet Service Provider من خلال المودم الموجود علي جهازك.

اسم أو كلمة Modem مأخوذة من كلمتين. الأولي Modulation ومعناها (تعديل) والثانية Demodulation ومعناها (إلغاء التعديل). ولتوضيح هذا المعني نقول. يتم تسجيل البيانات داخل ذاكرة الكمبيوتر في صورة رقمية (تسمي Binary) وتتكون هذه الأرقام عادة من (الواحد (1) والاصفار (0) تسمي بت (Bit) وحتي يمكن حمل هذه البيانات الرقمية (Digital) من جهاز الكمبيوتر بواسطة خط الهاتف القياسي يجب تحويلها. يطلق علي عملية التحويل من المعلومات الرقمية (المخزنة بالكمبيوتر) إلي القياسية (التي يفهمها الهاتف) اسم (تعديل) أو Modulate. عندما يتم تسلم معلومات قياسية علي مودم متصل بجهاز الخادم الخاص بمزود خدمة الانترنت، يجب تحويل البيانات من قياسية Analog إلي رقمية Digital مرة أخري يطلق علي هذه العملية اسم (إلغاء التعديل) أو Demodulate.

تتميز أجهزة المودم بأنها أكثر الأجهزة استخداماً في الاتصال بالانترنت وأقلها تكلفة ولكن يعاب عليها بطء سرعتها. ينقل المودم البيانات بسرعة ٣٣ كيلوبت في الثانية (33kbps)ويستقبل البيانات بسرعة ٥٦ كيلو بت في الثانية (56 KBPS) وهذا معناه أن أقصي كمية بيانات يمكن لجهاز المودم إرسالها في الثانية الواحدة عبر الاتصال التليفوني العادي هو ٥٦ ألف بت (56000 Bit). الواقع قد تفيد هذه السرعات في مشاهدة المواقع النصية أو التي تعرض صوراً بسيطة أما في حالة المواقع التي تعرض فيديو ورسوماً متقدمة، فتعتبر هذه السرعات بطيئة ولن تستطيع التعامل مع هذه المواقع بكفاءة. حتي تتمكن من

استخدام المودم يجب أن يكون لديك خط تليفوني وJack للهاتف بجوار جهاز الكمبيوتر .
عندما تتصل بالانترنت من خلال خط الهاتف فإن خط الهاتف يظل مشغولاً طوال الوقت ولن تتمكن من استخدامه للمكالمات الهاتفية العادية. حيث لا يمكن إجراء المكالمة والاتصال بالانترنت من خط واحد في نفس الوقت

الاتصال من خلال تقنية الـــــ DSL

كلمة **DSL** من أشهر المصطلحات المستخدمة مع الانترنت وكثيراً ما تسمعها وترددها وهي مأخوذة من العبارة **Digital Subscriber Line** ومعناها "خط مشترك رقمي".
وقد أحدثت هذه التقنية عند بداية ظهورها ثورة في تحقيق الاتصال بالانترنت، حيث تسمح باتصالات الصوت والبيانات عبر خطوط الهاتف العادية بسرعات تصل إلى ٧ميجا بت في الثانية (**7MBPS**). ولأن **DSL** يعمل من خلال خطوط الهاتف العادية، فيمكنك الاتصال بالانترنت بصفة مستمرة مع إجراء مكالمات هاتفية عبر نفس خط الهاتف.
هذه الخدمة غير موجودة في كل الأماكن حتي الآن ولكنها تأخذ في الانتشار بشكل سريع كل يوم، ولكنها محكومة ببعدك عن شركات التليفونات التي تقدم هذه الخدمة، فلا يجب أن تزيد المسافة عن ٢ ميل مما يشكل عائقاً في مد هذه الخدمة لكل الناس ، قد يمكن زيادة هذه المسافة باستخدام كابلات الألياف الضوئية **Optical Fiber** ولكنها ستزيد من تكلفة الخدمة .

تأتي أجهزة المودم التي تدعم تقنية **DSL** في نوعين الأول خارجي يتصل بجهازك عن طريق كارت الشبكة الموصل في جهازك أو بكابل **USB** أو كوحدة داخلية توضع في جهازك تستخدم هذه التقنية.

تقنية **DSL** خدمة هاتفية رقمية تعمل على خط الهاتف العادي. على الرغم من أن **DSL** يستخدم أساساً للاتصال بالانترنت لكل من مستخدمى المنازل والمؤسسات الصغيرة، إلا أنه يستخدم كذلك للاتصال البعيد بالانترنت ثم تولى أمر استراتيجيات ربط الشبكات عن بعد مثل **Virtual Private Networking** تختصر **VPN** ومعناها "ربط الشبكات الظاهرية الخاصة". سنشرح **VPN** فيما يلى من فصول الكتاب.

- **Cable Modem** : في هذه التقنية يتم بث بيانات الانترنت بسرعات عالية بنفس نظـــام إرسال إشارات محطات التليفزيون . وهذه التقنية غير مقيدة ببعد المسافة مثـــل تقنيـــة ISDN وDSL ولكن عيب هذه التقنية هو انخفاض سرعة تبادل البيانـــات في ســـاعات الذروة عند استخدام العديد من المستخدمين لهذه الخدمة في نفس الوقت. وبوجه عـــام تحتاج Cable Modem خارجي للعمل علي هذه التقنية يتصل بجهازك عـــن طريـــق كارت شبكة أو كابل USB .

يتميز الاتصال بالكابلات أو DSL بالمزايا الآتية على الاتصالات الهاتفية العادية التى شرحناها فى البند السابق .

السرعة:

تزيد سرعة اتصال الكابل عن سرعة الاتصال الهاتفي بما يعادل من عشرة إلى مائتي مرة. وذلك تبعا للخدمة المستخدمة. لخدمة اتصال DSL نفس سرعة الكابل. الفرق بينهما هو أن DSL عبارة عن خط استقبال مخصص بينما يشترك فى الكابل العديد من المستخدمين. ربما تنخفض السرعة فى حالة اتصال الكابل عندما يزيد عن المستخدمين (المشتركين) له فى نفس الوقت.

الاتصال الدائم بالانترنت:

فى حالتى الاتصال بالانترنت باستخدام الكابل أو DSL لن تحتاج إلى الاتصال ثم إنهاء الاتصال فى كل مرة تدخل فيها إلى الانترنت. وبالتالى لن تنتظر حتى ينتهى المودم من الاتصال بمزود الخدمة.

عدم انشغال الخط التليفونى

فى حالة استخدام الكابل، يتم الاتصال بالانترنت عبر كابلات التليفزيون بدلا من كابلات الهاتف. وعند استخدام DSL يتم تثبيت خط هاتفى منفصل لخدمة DSL. وبالتالى لن يتأثر خط التليفون العادى بالاتصال بالانترنت.

وفى مقابل هذه المزايا تضطر لدفع اشتراك أكبر. وتتوقف تكلفة خدمة DSL على سرعة الاتصال التى تختارها

تقنية ISDN

كلمة **ISDN** مأخوذة من العبارة **Integrated Services Digital Network** ومعناها(خدمة شبكة رقمية متكاملة). تقنية **ISDN** تعمل علي خطوط الهاتف الرقمية **Digital** وليست التناظرية **Analog** وهي تقنية قديمة وكانت تسمح بإرسال البيانات بضعف سرعة إرسالها على خط الهاتف العادي أي ١٢٨ كيلوبت فى الثانية بدلا من ٥٦ كيلو بت فى الثانية. يمكن تقسيم خط **ISDN** إلى قناتين منفصلتين مما يسمح بإجراء مكالمات هاتفية أثناء اتصال الجهاز بالانترنت

وبالطبع فإن تكلفة هذه الخدمة تكون أعلى من تكلفة خدمة خط الهاتف لأنها توفر سرعة أكبر. هذا بخلاف الرسوم التى تحصلها شركة الاتصالات مقابل تثبيت خط **ISDN**.

خطوط اتصال T1 و T3 السريعة

إذا كنت تعمل فى مؤسسة كبيرة ويهمك بصفة أساسية سرعة الاتصال فإن الاتصال بالانترنت عن طريق خطوط **T1** أو **T3** السريعة هو الحل المناسب لك. حيث يتم الاتفاق مع شركة الاتصالات التى تتبعها على تأجير خط رقمي مخصص ذو سرعة عالية.ولأن تكلفة هذا النوع من الاتصال عالية فإننا ننصح باستخدامه من قبل المؤسسات الكبيرة التى يزيد فيها عدد المستخدمين الذين يتصلون بالانترنت.

خطوط اتصال **T1** و **T3** عبارة عن خطوط خاصة سريعة فلا يشترك أى مستخدم خارجي فى الخط الذي تقوم بتأجيره. ولذلك فهي تستخدم أساسا في شبكات **WANs** (الشبكات الموسعة) الخاصة بالشركات الكبيرة.

تصل سرعة خط اتصال **T1** إلى ١٥٤٤ميجا بت فى الثانية **(1544 MBPS)**. يمكن لعدد من المستخدمين يصل إلى ٢٤ مستخدم الاشتراك فى خط **T1**. و تصل سرعة كل من المشتركين بالانترنت إلى ٦٤ كيلو بت فى الثانية **(64 MBPS)** وهى تقريبا مساوية للسرعة التي يتم الحصول عليها عند تخصيص خط تليفوني وجهاز مودم لكل مستخدم يعمل بسرعة ٥٦ كيلو بت فى الثانية. ولكن كلما قل عدد المستخدمين كلما ارتفعت سرعة الاتصال.

أما خط اتصال T3 فان سرعته أعلى من سرعة خط T1 حيث يصل معدل نقل البيانات باستخدامه إلى ٤٤١٨٤ ميجا بت فى الثانية (44184MBPS). ويمكن تقسيم كل خط من خطوط T3 إلى ٢٨ خط من خطوط T1. وبما أن خط T1 يخدم حتى ٢٤ مستخدم، فإن T3 يخدم ٦٧٢ مستخدم (٢٨X٢٤) وبالطبع فإن رسوم استخدام خطوط T3 لابد أن تكون أعلى من خطوط T1.

فى الشركات التى لا يستدعى عدد الموظفين فيها تأجير خط T1أو T3 كامل يمكن استئجار جزء من الخط فى هذه الحالة، يمكن الحصول على اتصالات بسرعة تتراوح من ١٢٨ إلى ٧٦٨ كيلو بت فى الثانية فى حالة استخدام خط اتصال T1وما يتراوح من 406 إلى 32 ميجا بت فى الثانية فى حالة T3.

- *خدمة الأقمار الصناعية* ***Satellite Service*** : في هذه الخدمة تستخدم إشارات الميكروويف وتوفر سرعات عالية جداً لتبادل البيانات وهي موجودة بنوعين إما **Unidirectional** (أحادي الاتجاه) أي يتم الاستقبال بسرعات عالية لموجات الميكروويف، أما الإرسال فيتم عبر خطوط الهاتف بسرعات بطيئة نوعاً ما ، والنوع الآخر هو **Bidirectional** (ثنائي الاتجاه) أي يتم الإرسال والاستقبال من خلال إشارات موجات الميكروويف ولكن عيب هذه التقنية أنها تتأثر بالأحوال الجوية فالرياح والثلوج تؤثر علي سرعة وجودة تناقل البيانات وقد تؤدي إلي قطع الاتصال .
- *الاتصال اللاسلكي* ***Wireless*** : تنتشر هذه الخدمة كثيراً في الأماكن العامة كالمطاعم والمراكز التجارية وهي تقوم علي تحقيق الاتصال اللاسلكي بالانترنت عن طريق جهاز بث لاسلكي يستطيع المستخدم الاتصال به الدخول علي الانترنت بسرعة 1Mbps .

المشاركة فى اتصال الانترنت

بعد أن تحدد طريقة الاتصال بالانترنت سواء كانت الاتصال الهاتفى أوDSL أو الكابل أو خطوط الاتصال المخصصة. يجب أن تقوم بإعداد الاتصال بحيث يشترك فيه أكثر من مستخدم على الشبكة.

تعتبر سمة ICS (Internet Connection Sharing) واحدة من الطرق المستخدمة لمشاركة الاتصال بالانترنت، وهى سمة موجودة فى نظام Windows. بواسطة هذه السمة لا يتم الاتصال المباشر بالانترنت إلا لجهاز واحد يعرف باسم بوابة الاتصال، الذى قد يكون اتصال هاتفى أو اتصال DSL. و يتم اتصال بقية الأجهزة على الشبكة بالانترنت عن طريق هذا الجهاز. وبذلك يمكن أن يتصفح أكثر من مستخدم الويب أو يقرأون رسائل البريد الالكتروني التى تصل إليهم فى نفس الوقت .

ولذلك يجب تشغيل بوابة الاتصال قبل أن تحاول الأجهزة الأخرى الاتصال بالانترنت من خلال سمة ICS.

اختيار متصفح الانترنت Internet Explores

الهدف النهائي من اتصال الشبكة الداخلية (LAN) للشبكة الانترنت العالمية، أن يتاح لجميع مستخدمي الشبكة تصفح الويب. و يتم ذلك من خلال أحد برامج تصفح الويب.

من أشهر برامج تصفح الانترنت برنامج Internet Explorer الموجود فى نظام لتشغيل Windows وبرنامج Netscape Navigator . برنامج Navigator موجود فى مجموعة من منتجات الانترنت المعروفة باسم Communicator .

يحتوى كل من البرنامجين على مجموعة برامج وأدوات تتعدى حدود تصفح الويب ومنها:-

- برنامج البريد الالكترونى الشهير Outlook Express .
- برنامج الدردشة عبر الانترنت MSN Messenger .
- برنامج إجراء الاتصالات بالصوت والصورة على شبكة الانترنت Netmeeting.

يأتي برنامج Internet Explorer ضمن نظام التشغيل Windows . بينما يتم تنزيل برنامج Communicator من موقع شركة Netscapeعلى الويب وعنوانه WWW.Netscape.Com وننصح باستخدام نفس البرنامج على جميع أجهزة الشبكة ليسهل عليك حل المشكلات التي قد تظهر لك في اتصالات الانترنت.

بعد إنشاء الشبكة ووصلها بشبكة الانترنت واختيار متصفح الويب واختيار عنوان لموقعك على الشبكة. يجب وضع نظام لتامين الشبكة حتى لا يتمكن شخص من خارج

الشبكة إلى التسلل إليها من خلال الانترنت .

لذلك فإن تطبيق إجراءات أمنية على الشبكة بأكملها يصبح امراً حتميا في حالة اتصال أي جهاز كمبيوتر في شبكتك بالانترنت. فيما يلى بعض الاقتراحات المفيدة في هذا الشأن. (راجع الباب السادس الخاص بأمان الشبكات لتتعرف علي نظم الأمان في شبكتك).

ملخص الفصل

تناولنا في هذا الفصل أهم طرق الاتصال بين الشبكة الداخلية وشبكة الانترنت. يجب أن تختار الطريقة التي تناسب حجم شبكتك وطبيعة عملك. ففي حين تناسب تقنية مثل تقنية DSL الشركات الصغيرة، يلزم الشركات الكبيرة التي يهمها سرعة الاتصال تأجير خطوط T1 و T3 السريعة. أما تقنية Dial-Up فإنها بطيئة جداً ولا تصلح لتنزيل الملفات الكبيرة .

تدريبات

١. اختر الإجابة الصحيحة

أ. تعتبر تقنية Dial-Up تقنية سريعة جداً .

ب. تستخدم تقنية DSL خط الهاتف العادي ورغم ذلك فهي أسرع من Dial-Up.

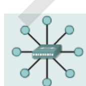
ج. تناسب تقنية خطوط اتصال T1 و T3 مستخدمي المنازل والمؤسسات الصغيرة.

د. زاد انتشار تقنية الاتصال اللاسلكي وهي تعمل بسرعة عالية ولا تتطلب جهاز بث لاسلكي .

٢. صل الإجابة الصحيحة

طريقة الاتصال بالانترنت	الوصف
١. الاتصال اللاسلكي Wireless	أ. تستخدم إشارات الميكروويف وتوفر سرعات عالية جداً لتبادل البيانات.
٢. الاتصال من خلال الهاتف Dial-UP	ب. تنتشر في الفنادق والمراكز التجارية

			وتحقق الاتصال بسرعة عالية.
٣.	خدمة الأقمار الصناعية Satellite Services	ج.	تكلفة هذا النوع من الاتصال عالية، ولذلك فلا تستخدمه سوي المؤسسات الكبيرة الذين يزيد فيها عدد المستخدمين الذين يتصلون بالانترنت.
٤.	خطوط T1 و T3	د.	تقنية بطيئة جداً ولا تصلح إلا للمستخدمين في المنازل والذين لا يحتاجون لتنزيل بيانات ذات حجم كبير أو لا يهمهم السرعة.



الباب الخامس

ربط شبكات Microsoft

*الفصل الرابع عشر : إعدادات شبكات **Windows Vista***

الفصل الخامس عشر : الاتصال بالشبكات

الفصل السادس عشر : مشاركة موارد الشبكة

الفصل الرابع عشر

إعداد شبكة

Windows Vista

ابتداء من **Windows 98** أتاحت ميكروسوفت لعملائها توصيل أجهزتهم المكتبية في شبكة من نوع نظير بنظير عن طريق نظم تشغيل سطح المكتب مثل **Windows XP** أو **Windows Vista**. بدون الحاجة إلي نظم تشغيل الشبكات الذي يستخدم مع شبكة من نوع **Client / Server** "وحدة الخدمة / العميل" ومن أمثلته **Windows Server 2000/2003/2008**. وفي هذا الفصل والفصلين التاليين ستتعرف علي كيفية ربط شبكات **Microsoft** باعتبارها واحدة من أشهر الشبكات المستخدمة. بالانتهاء من هذا الفصل ستتعرف علي :

- أنواع الشبكات في **Windows Vista**
- إعداد شبكة في **Windows Vista**
- كيفية توصيل البروتوكولات والخدمات التي تحتاجها الشبكة

أنواع الشبكات في Windows Vista

تدعم **Windows Vista** العديد من أنواع الشبكات وتتعامل مع جهازك علي أنه جهاز يقوم بأحد الأدوار التالية :

- جهاز مستقل يستطيع التعامل مع الشبكة عن طريق كارت المودم أو الانترنت، وخير مثال علي ذلك هو الجهاز المحمول **Laptop** المستقل الذي يستطيع الدخول علي شبكة المكتب أو الشركة مع أنه ليس عنصراً من هذه الشبكة ، كما تدعم **Windows Vista** السرية لتأمين شبكة المكتب عند اتصالها بالانترنت عن طريق مفهوم **Virtual Private networking (VPN)** "الشبكة الخاصة التخيلية" وهي عبارة عن شبكة تخيلية يتم إنشائها من خلال الانترنت. الجهاز الذي يقوم بهذا الدور يطلق عليه اسم **Remote workstation** "محطة عمل عند بعد" .
- الجهاز الموجود في شبكة صغيرة بدون وحدة مركزية **Server** يسمي **Workgroup Computer** "جهاز في مجموعة عمل" ويظهر هذا الدور في الشبكات من نوع **Workgroup** "مجموعة العمل" أو **Peer-to-Peer** "النظير للنظير" وتلك هي الأنواع المعتادة للشبكات المكتبية الصغيرة أو المنزلية.
- أن يكون الجهاز واحداً من مجموعة من الأجهزة (عشرات أو مئات) يعملون تحت إشراف واحد أو أكثر من الأجهزة المركزية يعملون بنظام التشغيل **Windows Server** ، وتقوم هذه الوحدات المركزية بتنظيم قوائم أسماء وحسابات المستخدمين وكلمات المرور ، في هذه الحالة يسمي الجهاز الذي يعمل بنظام التشغيل **Windows Vista** باسم **Domain member** أو عضو في شبكة ميدانية **Domain Network** .
- يكون الجهاز عبارة عن عضو في شبكة من نوع **client/server** "الخادم/العميل" التي بدورها يمكنها أن تتعامل مع شبكة أخري مجاورة لها (مثال علي ذلك شبكة فرع ما في شركة تستخدم شبكة أكبر) في هذه الحالة يطلق علي الجهاز اسم عضو

Domain member في شبكة من نوع Enterprise Network .

تدعم بعض نسخ Windows Vista جميع أنواع الشبكات بينما لا تدعم بعض الطبعات أنواع أخري . كما في الجدول التالي :

Enterprise	Domain	Workgroup	Remote VPN	
		✓		Home Basic
		✓		Home Premium
✓	✓	✓	✓	Business
✓	✓	✓	✓	Enterprise
✓	✓	✓	✓	Ultimate

الشئ الوحيد الذي لا يستطيع الجهاز الذي يعمل بنظام Windows Vista أداؤه، هو القيام بدور الوحدة المركزية أو الخادم في الشبكات من النوع Domain "الميدان" أو Enterprise ففي هذه الحالات قد تحتاج إلي جهاز واحد علي الأقل يقوم بوظيفة الوحدة المركزية Server ويعمل علي طبعات Windows من نوع Windows Server .

تدعم Windows Vista خدمة مشاركة الملفات حتي ٥ أو ١٠ أجهزة (٥ للنسخة من نوع Home و ١٠ للنسخة من نوع Ultimate أو Enterprise) فإذا كنت تريد مشاركة الموارد علي عدد أكبر من ١٠ أجهزة فعليك تثبيت نسخة من نوع Windows Server

إعداد شبكة في Windows Vista

نتعرض معك في هذا الفصل لإعداد الشبكة من النوع Peer-To-Peer "نظير لنظير" وهي من أبسط أنواع الشبكات التي يمكنك بناءها أما إذا أردت التعرف علي طرق بناء الأنواع الأخرى المتقدمة من الشبكات فيجب مراجعة باقي فصول الكتاب.

إذا كانت الأجهزة والكابلات وكروت الشبكة مثبتة لديك بشكل صحيح فما عليك الآن سوي تكوين الشبكة في Windows Vista لتجعل الأجهزة تتعرف علي بعضها

لتبادل البيانات .

عندما تكون كروت الشبكة مثبتة في الأجهزة ومثبت معها برامج التشغيل **Drivers** الخاصة بالكروت ، تتعرف **Windows Vista** علي الكروت حسب مفاهيم التوصيل والتشغيل الحديثة (**Plug and Play**) ولكن ينقصك التعرف علي البرامج والبروتوكولات التي تحتاجها **Windows** لتكوين الشبكة وإضافة هذه البرامج.

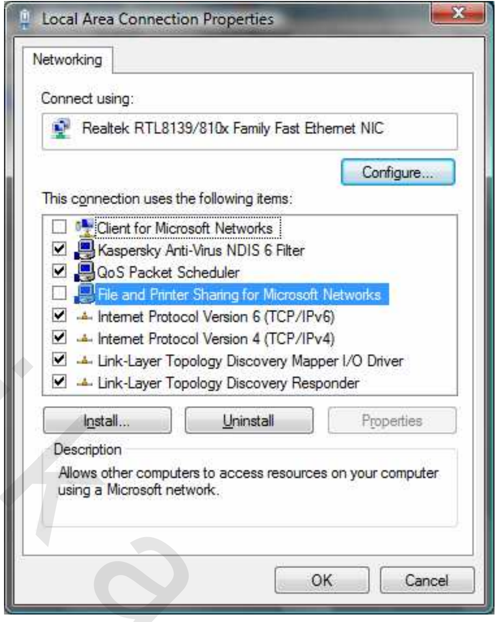
لتوصيل البروتوكولات والخدمات التي تحتاجها تابع الخطوات التالية :

١. تأكد من دخولك إلي الجهاز بحساب مدير أو مسئول **Administrator**، انقر قائمة **Start** "ابدأ"، ثم اختر **Control Panel** ، ثم انقر الارتباط **Network and Internet** "الشبكة والانترنت" ثم انقر **Network and Sharing Center** "مركز الشبكة والمشاركة" .

٢. من قائمة المهام في الناحية اليسري من النافذة (أو جهة اليمين عند تغيير اتجاه الشاشة من اليمين إلي اليسار) ، انقر الارتباط **Manage Network Connection** "إدارة اتصالات الشبكة".

٣. بزر الماوس الأيمن انقر **Local Area Connection** ومن القائمة التي ستظهر اختر **Properties** "خصائص".

٤. عندما يظهر مربع **User Account Control** "التحكم في حساب المستخدم" إذا كنت مسجلاً دخولك كمسئول انقر **Continue** "متابعة"، والإ أدخل حساب أحد المسئولين ثم انقر **OK** "موافق" سيظهر المربع الحواري **Properties** "متابعة" ويظهر فيه اسم كارت الشبكة المثبت علي جهازك في خانة **Connect Using** "الاتصال باستخدام" شكل ١٤-١.



شكل ١٤–١ مربع خصائص الشبكة المحلية

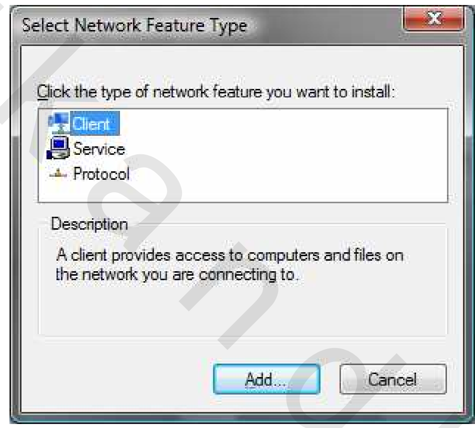
٥. ستلاحظ تنشيط بعض الخيارات في تلك القائمة بشكل افتراضي ولكن هناك اختيارات أساسية يجب عليك التأكد من تنشيطها لتفي بحاجات الشبكات الصغيرة التي نتحدث عنها ومن هذه العناصر ما يلي :

- **Client for Microsoft Networkers** : يسمح لجهازك باستخدام موارد المشاركة كالمجلدات والطابعات من أجهزة الكمبيوتر الأخرى في الشبكة.
- **File and Printer Sharing for Microsoft Networks** : يسمح لك بمشاركة مواردك مع الأجهزة الأخرى في الشبكة (إذا كنت لن تحتاج لمشاركة مجلدات أو طابعات من جهازك علي الشبكة فيمكنك إلغاء تنشيط هذا الاختيار) وقد يفيدك هذا في حماية جهازك من مشاركة موارده حتي لو عن طريق الخطأ.
- **QoS Packet Scheduler** : تستخدم لبعض الشبكات لكي تنظم أولويات تزاحم البيانات في الشبكة وقد لا تحتاجها في حالة الشبكات الصغيرة.
- **Internet Protocol (TCP/IP)** : للتأكد من وجود البروتوكول TCP/IP

وهو البروتوكول المسئول عن تعريف كل خدمات الانترنت وكذلك مشاركة المجلدات والطابعات (الموارد) علي الشبكة، وستلاحظ ظهور إصدارين ننصحك بتنشيط الإصدارين.

إذا أردت إضافة عناصر أخري بالإضافة إلي العناصر المحددة، أو إذا حذفت أحد هذه العناصر عن طريق الخطأ وتريد تثبيته مر أخري تابع الخطوات التالية:

١. انقر زر **Install** "تثبيت" ، سيظهر المربع الحواري **Select Network Feature Type** "تحديد نوع ميزة الشبكة" . شكل ١٤-٢



شكل ١٤-٢ المربع الحواري **Select Network Feature Type** "تحديد نوع ميزة الشبكة"

٢. من هذا المربع الحواري اختر نوع العنصر الذي تريده سواء كان **Client** "عميل" أو **Service** "خدمة" أو **Protocol** "بروتوكول" ثم انقر **Add** "إضافة".

٣. عند اختيار أي نوع والنقر علي **Add** "إضافة" سيظهر مربع حواري آخر يحتوي علي العناصر الخاصة بهذا النوع للاختيار منها ، اختر العنصر الذي تريد تثبيته ثم انقر **OK** "موافق" .

تهيئة بروتوكول TCP/IP

بعد تشبيك أجهزة الشبكة بالطريقة الصحيحة وإعداد كروت الشبكة علي الأجهزة بطريقة صحيحة يجب عليك التأكد من وجود عنوان **IP Address** لكل جهاز كمبيوتر

(وهو عنوان مميز أو اسم مميز لكل جهاز يعرف به خلال الشبكة) وهذا العنوان يعرف لأي جهاز كمبيوتر في الشبكة عن طريق إحدي الطرق التالية:

- إذا كانت الشبكة بها جهاز يستخدم Windows Internet Connection Sharing لمشاركة الاتصال بالانترنت، أو كان مثبت في الشبكة جهاز Router "موجه" ، أو إذا كانت شبكتك المحلية LAN تستخدم خادم من نوع Windows 200x Server ، فكل جهاز في هذه الحالات سيحصل علي عنوان خاص له IP أتوماتيكياً عن طريق جهاز الموجه Router أو الخادم Server في الشبكة الذي يعمل بالبروتوكول (DHCP) Dynamic Host Configuration Protocol، ويقوم بإعطاء الأجهزة عناوين بشكل ديناميكي غير ثابت ، لذا ننصحك بوضع جهاز موجه Router في شبكتك حتي وإن لم تحتاج الموجه Router للدخول علي الانترنت.
- يمكنك إعطاء كل جهاز في الشبكة عنوان مميز له يدوياً ويسمي في هذه الحالة عنوان ثابت Static Address .
- إذا لم تتوفر أي طريقة من الطرق السابقة تقوم Windows بإعطاء عناوين لأجهزة الشبكة ولكن هذا قد يبطئ النظام.

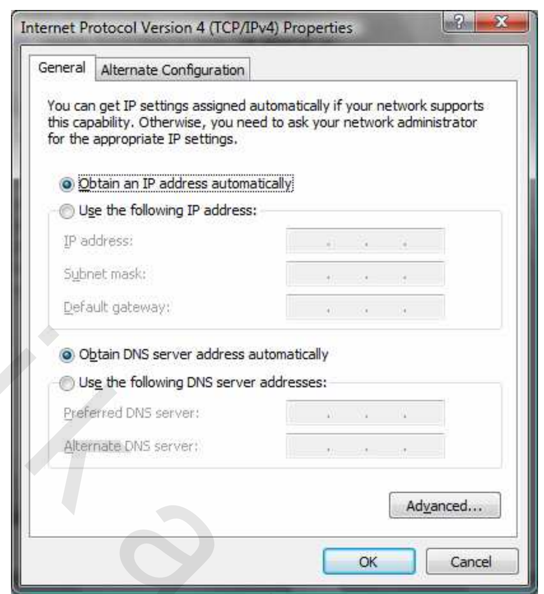
إذا قمت بإضافة جهاز جديد للشبكة عليك التأكد من أن الشبكة معدة بطريقة صحيحة بعد الجهاز الجديد الذي أضيف .

للتأكد أن الشبكة أعدت بطريقة صحيحة تابع الخطوات التالية:

١. تأكد انك تعمل علي الجهاز كمديرِ Administrator أو أعد الدخول علي الجهاز مرة أخري ثم تابع نفس خطوات التمرين السابق حتي تفتح نافذة Properties الخاصة بالشبكة المحلية LAN (راجع شكل ١٤-١).

٢. انقر الاختيار Internet Protocol Version 4(TCP/IP) ثم انقر زر Properties "خصائص" أسفل النافذة .

٣. ستظهر نافذة خصائص البروتوكول **IP** كما في شكل ١٤–٣.



شكل ١٤–٣ خصائص البروتوكول **IP**

٤. تأكد أن الخيار **Obtain an IP address automatically** "الحصول علي عنوان **IPv** تلقائياً" محدداً حتي يحصل الجهاز الجديد في الشبكة علي العنوان المناسب له ، أو قم بإدخال العنوان المعطي من مزود الخدمة الخاص بك **(Internet Service Provider) ISP** أو مدير الشبكة.

٥. إذا لم تتوفر عندك هذه العناوين وتريد إعطاء الأجهزة عناوين في الشبكة، أدخل بيانات الخانات علي النحو التالي:

- قم بتنشيط الخيار **Use the following IP address** "استخدام عنوان **IPv** التالي" .
- في خانة **IP address** "عنوان **IP**" أدخل البيانات كالتالي **192.168.0.x** مع استبدال الحرف **x** بالرقم الذي تختاره وتحدده لأي جهاز كمبيوتر علي الشبكة.
- في خانة **Subnet Mask** "طول بادئة الشبكة الفرعية" أكتب **255.255.255.0**.

- اترك الخانة **Default Gateway** "العبارة الافتراضية" خالية.
- تأكد من تنشيط خانة الاختيار **Obtain DNS Server Address Automatically** "الحصول علي عنوان خادم **DNS** تلقائياً" .

تهيئة TCP/IP يدوياً

عادة يكون البروتوكول **TCP/IP** هو الشئ الوحيد الذي يجب عليك تهيئته يدوياً ، فإذا كانت شبكتك تعمل بنظام برتوكول **Dynamic Host Configuration Protocol (DHCP)** ففي هذه الحالة سيتم ضبط برتوكول **TCP/IP** تلقائياً من الأجهزة المستخدمة في تكوين الشبكة كالموجهات **Routers** أو أجهزة المشاركة الأخرى . أما إذا كانت شبكتك صغيرة ولا تحتوي علي خادم يعمل بنظام **DHCP** أو أي جهاز مشاركة يقوم بضبط بروتوكول **TCP/IP** ، يمكنك ترك **Windows** تقوم بوظيفة تهيئة هذا البروتوكول نيابة عنك.

إذا كان جهازك جزء أو عضو في شبكة محددة العناوين **IP Addresses** كشبكة محلية **LAN** في شركة ما، ففي هذه الحالة يجب أن تضبط معلومات العنوان **IP** بشكل يدوي وإدخال البيانات التالية بعد أن تكون قد حصلت عليها من مدير الشبكة.

- **IP Address**
- **Subnet Mask**
- **Default gateway**
- **DNS domain name**
- **Preferred DNS servers**

اختيار مكان الشبكة

يفيدك تحديد مكان الشبكة خصوصاً إذا كان لديك جهاز محمـــول **Laptop** وتريـــد أن تدخل لشبكةً ما أو لشبكة الانترنت من أي مكان أنت متواجد فيه، فعندما تدخل علـــي شبكة ما يحثك **Windows** علي اختيار مكان الشبكة الـــتي قمـــت بالـــدخول عليهـــا وستتوقف إعدادات حائط الصد الناري **Firewalls** والسرية **Security** علـــي مكـــان ونوع الشبكات التي دخلت عليها، فعلي سبيل المثال يكون مطلوب مستوي عـــالٍ مـــن

السرية إذا دخلت علي شبكة في مطار مثلاً بينما ينخفض مستوي السرية إذا دخلت علي شبكة في بيت أو مكتب.

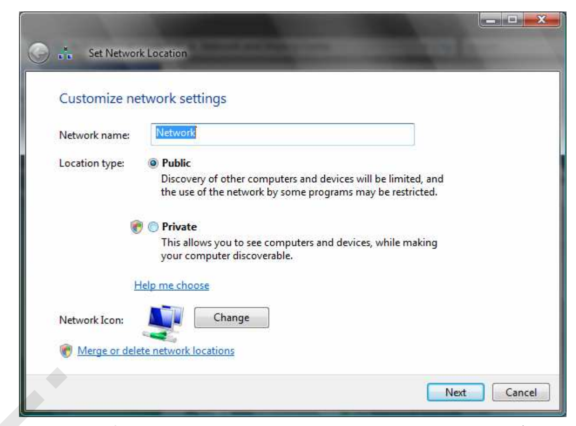
يمكنك اختيار موقع أو مكان الشبكة من ثلاث اختيارات **Home** أو **Work** أو **Public** يمكنك اختيار **Home** أو **Work** إذا كنت تتصل أو تدخل علي شبكة موثوق بها ولا يكون لديك مجال للقلق عندما يري أحد من مستخدمي هذه الشبكة ملفات وموارد المشاركة علي جهازك ، واختر الموقع **Public** عندما تكون غير واثق في الشبكة التي تدخل عليها مثل الشبكات الموجودة في المقاهي والفنادق العامة فهذه الأماكن يجب أن تكون مستوي السرية الموجودة علي جهازك عالٍ حتي لا يتمكن أحد مستخدمي الشبكة من رؤية جهازك والعبث في بياناته.

عندما تنتقل بجهازك من مكان إلي آخر سيستشعر **Windows** التغيير في الشبكة ويحثك علي تحديد مكان ونوع الشبكة التي دخلت عليها لكي يضبط مستوي السرية التي يتعامل بها مع الشبكة .

لتغيير موقع الشبكة التي ستدخل عليها تابع الخطوات التالية:

١. من قائمة **Start** "ابدأ" انقر **Network** "الشبكة" ثم اختر **Network and Sharing Center** "مركز الشبكة والمشاركة" . ستظهر نافذة **Network and Sharing Center** "مركز الشبكة والمشاركة" .

٢. من يمين النافذة انقر الارتباط **Customize** "تخصيص" ، سيظهر المربع الحواري **Set Network Location** ضبط موقع الشبكة" . شكل ١٤-٤



شكل ١٤-٤ المربع الحواري Set Network Location

٣. اختر **Public** "عمومي" إذا كانت الشبكة التي ستدخل عليها غير موثوق بها أو في مكان عام، أو انقر **Privet** "خاص" إذا كانت الشبكة التي ستدخل عليها موثوق بها أو موثوق في مستخدميها لمشاركة ملفات ومجلدات المشاركة الخاصة بك بأمان.

٤. انقر **Next** "التالي" حتي يتم تحديد مكان الشبكة التي ستعمل عليها ثم انقر **Close** "إغلاق".

إعداد هوية جهازك

بعد الانتهاء من إعداد شبكتك يجب عليك التأكد من أن كل الأجهزة فيها تعمل علي نفس الشبكة أو الميدان أما إذا كان جهازك عبارة عن عضو في شبكة من نوع الميدان Domain فعليك أخذ هذه المعلومات من مدير الشبكة حتي تقوم بتعريف هوية جهازك .

إذا كان شبكتك يعمل بها أجهزة مثبت عليها نظام **Windows** وليس نظام **Windows 200x**. تابع الخطوات التالية:

١. افتح قائمة **Start** "ابدأ" ثم انقر **Computer** "الكمبيوتر" بزر الفأرة الأيمن ومن القائمة التي ستظهر اختر **Properties** "خصائص" ستظهر نافذة **Properties** "خصائص" .

٢. من الجزء **Computer Name, Domain, Workgroup Settings** "إعدادات اسم الكمبيوتر والمجـــال ومجموعـــة العمـــل" انقـــر **Change Settings** "تغـــيير الإعدادات" ، وعندما يظهر مربع **User Account Control** "التحكم في حساب المستخدم" إذا كنت مسجلاً دخولك كمسئول ثم انقـــر **Continue** "متابعـــة" وإلا أدخل كلمة مرور المسئول ثم انقر **OK** "موافق".

٣. تأكد أن كل كمبيوتر في الميدان الذي أنشأته يحمل اسماً مختلفاً عن باقي الأجهزة وأنـــه منتمي أو يعمل علي هذه الشبكة . إذا وجدت اختلافاً أو أن المعلومات تظهر بصورة غير صحيحة انقر زر **Network ID** .

٤. بمجرد النقر علي زر **Network ID** سيبدأ معالج الإعداد في العمل وطـــرح الأســـئلة عليك.

٥. وعليك الإجابة علي هذه الأسئلة لتعريف جهازك بـــشكل صـــحيح ، إذا اختـــرت **Home Use** "استخدام منزلي" سيعد المعالج جهازك علي أنه يعمل في شبكة **Peer-to-Peer** "نظير لنظير" لمجموعة عمل **Workgroup** ثم ينهي عملية الإعداد .

٦. أما إذا اخترت **Business** "عمل" فسيقوم **Windows** بإعداد المزيد من الـــسرية علي جهازك .

٧. ثم سيسألك المعالج إذا كان شركتك تستخدم شبكة نطـــاق أو ميـــدان **Domain** أو بدون ميدان فإذا كنت مرتبط بشبكة كبيرة تعمل علي النظـــام **Windows 200x** ، قم بتنشيط الخيار **With Domain** "بنطاق" . أما إذا كانت شبكتك صغيرة فـــاختر بدون **Without Domain** "بدون نطاق" .

٨. عندما يطلب منك المعالج تحديد اسم لشبكة العمل، اكتب الاسم الذي تريده ثم انقـــر **Next** "التالي" ثم **Finish** "إنهاء" لإنهاء عملية الإعداد.

تهيئة الحائط الناري Windows Firewall

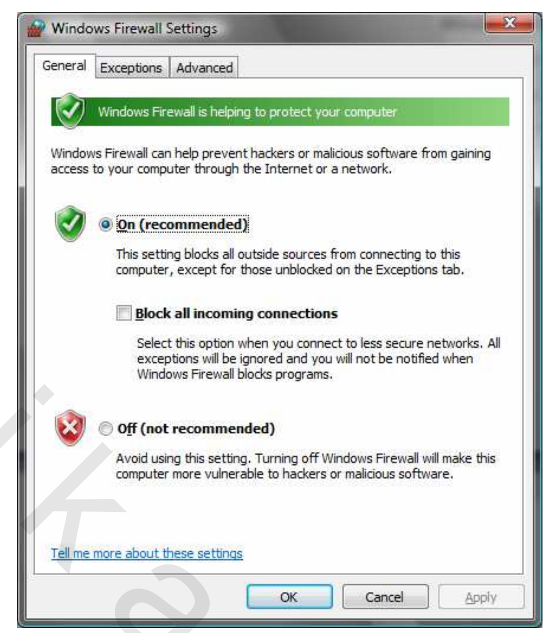
عند العمل علي شبكة من الأفضل أن تتأكد أن الحائط الناري **Firewall** الخـــاص بـــ **Windows** يعمل بصورة صحيحة حتي تحمي جهازك وملفات المـــشاركة الخاصـــة بـــك

وشبكتك كلها من أي هجوم قد تتعرض له . نتعرض في هذا الشرح لحماية جهازك بغض النظر عما إذا كان موجود علي الشبكة نظام حماية جيد لمواردها أم لا ، فهذه خطوات يجب عليك إتباعها للتأكد من أن **Windows** تعمل بصورة صحيحة وبأمان. تابع الخطوات التالية:

١. تأكد أنك تعمل علي الكمبيوتر كمسئول أو قم بإعادة تشغيل الجهاز وسجل دخولك كمسئول .

٢. افتح قائمة **Start** "ابدأ" ثم اختر **Control Panel** "لوحة التحكم" ثم انقر **Security** "الأمان" ثم انقر **Windows Firewall** "جدار حماية **Windows**" ثم انقر **Change Settings** "تغيير الإعدادات" .

٣. سيظهر أمامك المربع **Windows Firewall Settings** "إعدادات جدار حماية **Windows**" ويظهر التبويب **General** "عام" هو التبويب النشط، تأكد من أن خانة الاختيار **On(Recommended)** "تشغيل (مستحسن)" مختارة، مع ملاحظة عدم تحديد خانة اختيار **Block All Incoming Connection** "منع كافة الاتصالات الواردة" لاستخدام شبكتك لمشاركة الملفات والطابعات. شكل ١٤-٥.



شكل ١٤–٥ التبويب General "عام" داخل المربع الحواري Windows Firewall Settings "إعدادات جدار حماية Windows"

٤. قم بتنشيط التبويب Exceptions "استثناءات" وتأكد أن مربع الاختيار File and Printer Sharing نشطاً.

٥. افتح التبويب Advanced "خيارات متقدمة" ستلاحظ تنشيط الاختيار Local Area Network ويجب أن يكون أي اتصال آخر منشطاً إذا كنت تعمل علي أكثر من شبكة.

٦. انقر OK "موافق" لإغلاق المربع الحواري. إذا كان جهازك متصلاً بالانترنت عن طريق الشبكة LAN ، فتكون هذه الخطوات كافية للتأكد من أن جهازك يعمل بشكل صحيح ، أما إذا كان جهازك يتصل بالانترنت عن طريق جهاز مودم فلن يكون Windows Firewall كاف لحماية جهازك من العبث والسطو. ويجب عليك متابعة الخطوات التالية لحماية جهازك.

٧. افتح قائمة Start "ابدأ" ثم اختر Control Panel "لوحة التحكم" ثم اختر

"الــشبكة والانترنــت" ثم اختــر **Network and Internet** **Network and** **Sharing Center** "مركز الشبكة والمشاركة" .

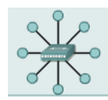
٨. تأكد أن مكان الشبكة **Network Location** مضبوط علي **Public Network** شبكة عامة" وهذا سيحمي أي ملفات أو طابعات مشتركة وبهذه الخطوات ســتتأكد أنك قمت بتأمين جهازك ضد أي عبث أو سطو ، قم بتكرار هذه الخطــوات لبــاقي أجهزة الشبكة وعند إذن يمكنك استخدام شبكتك بأمان.

ملخص الفصل

شرحنا في هذا الفصل أنواع الشبكات التي تدعمها **Windows Vista** ، وتعرضنا لإعداد شبكة من نوع **Peer – to Peer** "نظير /بنظير" وهي من أبسط أنواع الــشبكات الــتي يمكن بناءها. وهي عملية سهلة يتولاها **Windows Vista** عن طريق خطــوات ســهلة ومتسلسلة .

تدريبات

١. اتبع خطوات إعداد شــبكة **Peer – to – Peer** في **Windows Vista** ثم أطلــع مدربك علي نتيجة عملك.





نتعرف في هذا الفصل علي كيفية الاتصال بالشبكات وكيفية توصيل جهازك بمجموعة عمل، أو شبكة نطاق والوصول إلي جهازك عن بعد، كما ستعرف كيفية تخزين وإدارة كلمات مرور الشبكة.

بانتهاء هذا الفصل ستتعرف علي :

- ***توصيل كمبيوترك بمجموعة عمل***
- ***توصيل كمبيوترك بشبكة نطاق***
- ***الاتصال بمجال من مكان آخر***
- ***الوصول إلى كمبيوترك المجالي عن بعد***
- ***تخزين وإدارة كلمات مرور الشبكة***

توصيل كمبيوترك بمجموعة عمل

Workgroup Network "شبكة مجموعة العمل" تسمى أيضاً **Peer To Peer Network** "شبكة النظير للنظير" هي شبكة لا يوجد بها كمبيوتر مركزي (يسمى جهاز الخادم أو **Server**) يتحكم في باقي الأجهزة ويقوم بالتأكد من أسماء المستخدمين وكلمات مرور كل منهم.

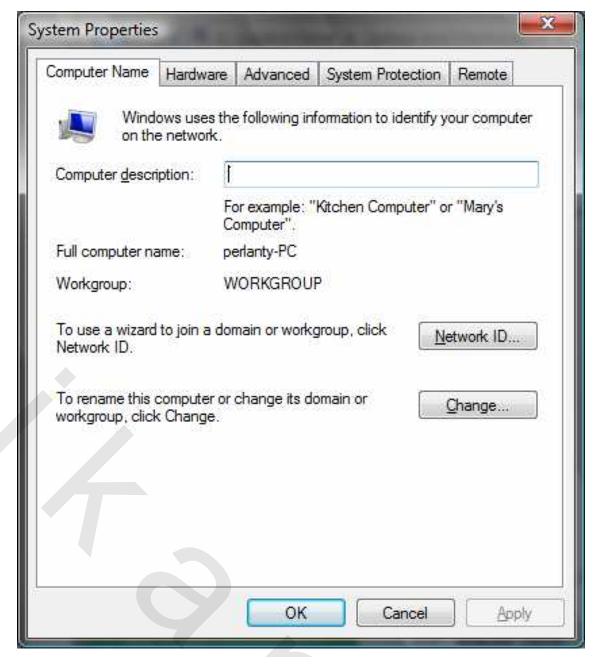
في هذه الشبكة يتولى كل كمبيوتر إدارة قائمة مستخدميه ونظام السرية الخاص بهم. بعبارة أخرى حسابات المستخدمين لكل كمبيوتر تدار فردياً، وتحتاج إلى حساب مستخدم في الكمبيوتر الذي تريد تسجيل دخولك إليه.

إذا كانت أسرتك تستعمل عدة كمبيوترات أو كنت تعمل في مؤسسة صغيرة تستخدم أقل من ١٠ أجهزة لكي يتمكنوا من مشاركة الموارد كالطابعات والمجلدات، ستكون غالباً جزءا من شبكة مجموعة العمل.

لكي تضم كمبيوترك إلى مجموعة عمل جديدة تابع الخطوات الآتية:

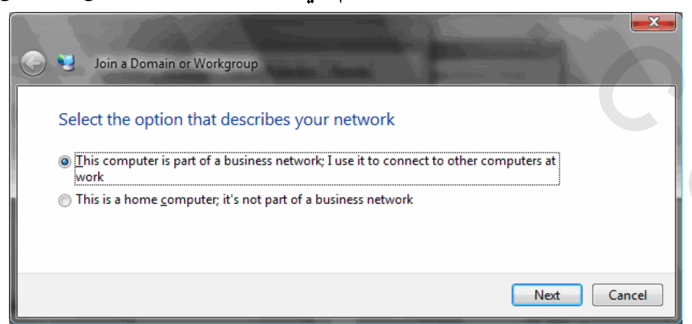
١. من لوحة التحكم، انقر **System and Maintenance** "النظام والصيانة"، ثم انقر **System** "النظام". تظهر نافذة **System** "النظام"، وبها معلومات عن كمبيوترك.

٢. تحت مجموعة **Computer name, domain and Workgroup Settings** "إعدادات اسم الكمبيوتر والمجال ومجموعة العمل"، انقر **Change Settings** "تغيير الإعدادات". عندما يظهر مربع الحوار **User Account Control** "التحكم في حساب المستخدم"، إذا كنت مسجلاً دخولك كمسئول، انقر زر **Continue** "متابعة"، وإلا، اكتب كلمة مرور المسئول، وانقر **OK** "موافق". يظهر مربع الحوار **System Properties** "خصائص النظام"، وتظهر تلقائياً علامة التبويب **Computer Name** "اسم الكمبيوتر". شكل ١٥-١



شكل ١٥-١ مربع System Properties "خصائص النظام"

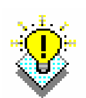
٣. على يمين To use a Wizard to Join a Domain or Workgroup "لاستخدام معالج للانضمام إلى مجال أو مجموعة عمل"، انقر الزر Network ID "معرف الشبكة". يبدأ معالج الاتصال بمجال أو مجموعة عمل. ويظهر مربع Join Domain or Workgroup "الانضمام إلي مجال أو مجموعة عمل". شكل ١٥-٢



شكل ١٥-٢ أو خطوة من خطوات معالج الاتصال بمجال أو مجموعة عمل

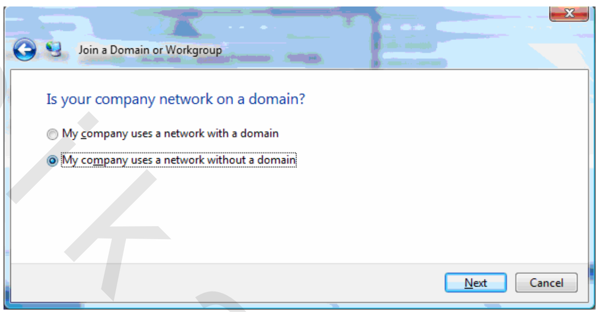
٤. تأكد من تنشيط الخيار This Computer is Part of a business Network

"هذا الكمبيوتر جزء من شبكة العمل"، ثم انقر الزر **Next** "التالي".



إذا قمت بتنشيط الخيار **This is a home computer** "هذا الكمبيوتر للاستخدام المنزلي" لن تتمكن من إنشاء مجموعة عمل جديدة.

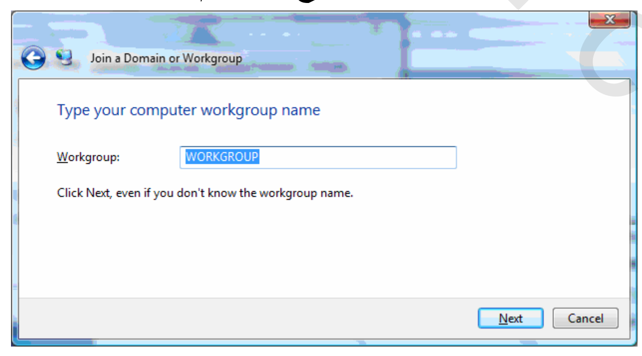
تظهر الشاشة التالية لتسألك هل توجد شبكة الشركة على مجال (شكل ١٥-٣).



شكل ١٥-٣ مربع تحديد إذا كانت الشبكة علي مجال

٥. نشط الخيار **My company uses a network without a domain** "تستخدم الشركة شبكة بدون مجال"، ثم انقر الزر **Next** "التالي". تظهر شاشة تطالبك بكتابة اسم مجموعة العمل. (شكل ١٥-٤).

٦. في المربع **Workgroup** "مجموعة العمل"، اكتب اسماً معبراً لمجموعة العمل الجديدة (مهما تكن الطريقة التي تكتب الاسم بها، سيظهر بأحرف كبيرة). ثم انقر الزر **Next** "التالي". تظهر آخر شاشة من شاشات معالج الانضمام إلى مجال أو مجموعة عمل.



شكل ١٥-٤ تحديد اسم للشبكة

٧. انقر الزر **Finish** "إنهاء"، لإنهاء المعالج والعودة إلي مربع الحوار **System Properties** "خصائص النظام".

٨. في مربع الحوار **System Properties** "خصائص النظام"، انقر **OK** "موافق".

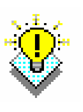
٩. أغلق كل البرامج والملفات المفتوحة، وعندما يظهر مربع الرسالة انقر الزر **Restart Now** "إعادة التشغيل الآن" وأعد تشغيل كمبيوترك لكي يسري مفعول التغيير.

١٠. بعد معاودة تشغيل، أعرض نافذة **System** "النظام"، وتحقق من أن كمبيوترك منضم الآن إلى مجموعة العمل الجديدة.

توصيل كمبيوترك بشبكة نطاق

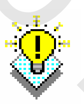
شبكة النطاق **Domain Network** هي على عكس شبكة مجموعة العمل تستخدم مع **Windows Server 200X** للتحكم في جميع أجهزة الشبكة.

ويتم تعريف حسابات المستخدمين على الجهاز الخادم الذي يتحكم في الشبكة وفيها يتم منح صلاحيات الوصول إلى ملفات وموارد الشبكة لبعض الأشخاص أو الإدارات أو المجموعات.



نستخدم عبارة **Windows Server 200X** للإشارة إلى **Windows Server 2008** أو **Windows Server 2003** أو **Windows Server 2000** أو **Windows Server NT 4.0**.

لكي تسجل دخولك إلى نطاق **(Domain)**، يجب أن يكون لديك حساب مستخدم للنطاق **(Domain Account)** محمي بكلمة مرور. ولذلك تستطيع أن تسجل دخولك من أي كمبيوتر موجود على النطاق.

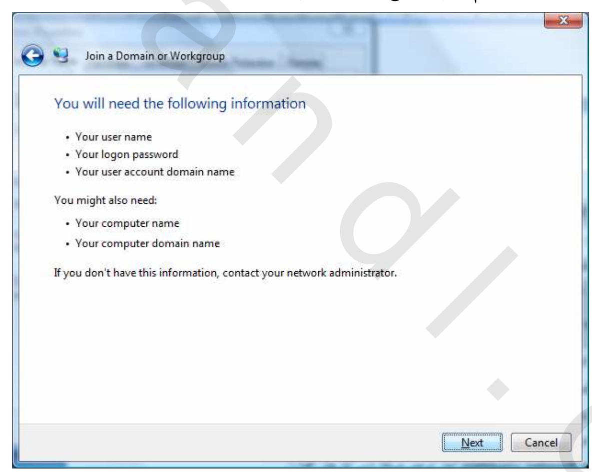


تذكر أن حساب مستخدم النطاق **(Domain Account)** غير حسابات مستخدمي ويندوز **(Windows Vista Accounts)** لكي لا تخلط بينهما.

لكل كمبيوتر في النطاق اسم مميز لا يشترك مع غيره من الكمبيوترات الموجودة في نفس المجال.

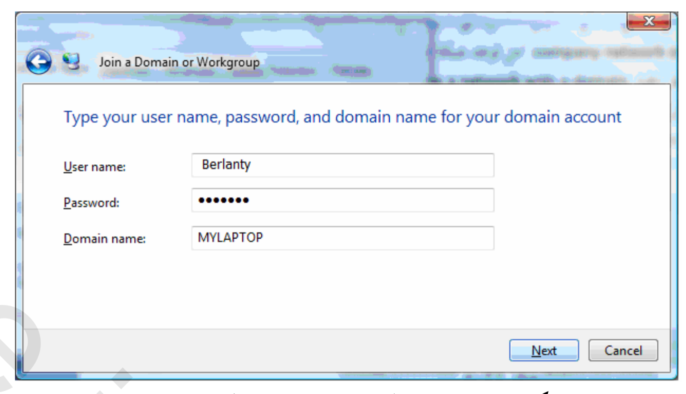
إذا كان لديك كمبيوتر خصص له حساب داخل مجال وتريد توصيله بالمجال اتبع الآتي:

1. **صل كمبيوترك بشبكة شركتك، إما مادياً أو من خلال اتصال VPN.**
2. **نفذ الخطوات من ١ إلي ٤ من التمرين السابق حتى تظهر أمامك الشاشة التي تسألك "هل توجد شبكة الشركة Is your company network on a domain على مجال". (شكل ١٥-٣ السابق)**
3. **تأكد من تنشيط الخيار My company uses a network with a domain "تستخدم الشركة شبكة ذات مجال"، ثم انقر الزر Next "التالي". يعرض المعالج قائمة بالمعلومات التي تحتاج إليها قبل المتابعة مثل اسم الكمبيوتر وكلمة المرور واسم مجال حساب المستخدم (شكل ١٥-٥).**



شكل ١٥-٥ تحديد المعلومات المطلوبة للشبكة

4. **تأكد أنك تملك كل المعلومات الضرورية، ثم انقر الزر Next "التالي". تظهر شاشة تطالبك بكتابة اسم المستخدم وكلمة المرور. (شكل ١٥-٦)**

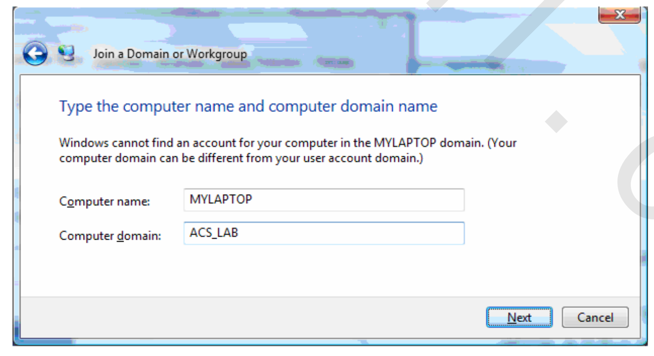


شكل ١٥–٦ إدخال اسم المستخدم وكلمة المرور

٥. اكتب اسمك وكلمة مرورك واسم المجال. مهما تكن الطريقة التي تكتب اسم المجال بها، سيظهر بأحرف كبيرة.

٦. انقر الزر **Next** "التالي". يبحث **Windows Vista** في المجال المحدد عن حساب كمبيوتر بنفس اسم كمبيوترك ويعرض رسالة إذا عثر على واحد.

إذا لم يعثر **Windows** على كمبيوتر ومجال بالاسم المحدد سيعرض عليك شاشة تطالبك بكتابة اسم الكمبيوتر واسم المجال (شكل ١٥–٧). اكتب اسم الكمبيوتر واسم المجال ثم انقر زر **Next** "التالي".



شكل ١٥–٧ تحديد اسم كمبيوترك واسم المجال

٧. انقر **Yes** "نعم". رداً على الرسالة التي تخبرك أن ويندوز عثر على حساب باسم الكمبيوتر، يسألك **Windows Vista** إن كنت تريد تمكين حسابك على

الكمبيوتر.

٨. إذا كنت تريد تمكين حسابك، انقر الزر **Next** "التالي". وإلا، نشط الخيار **Do Not add a domain user account** "عدم إضافة حساب مستخدم المجال الآن"، ثم انقر الزر **Next** "التالي".

يسألك **Windows Vista** إن كنت تريد الحصول على امتيازات مسئول في هذا الكمبيوتر. ما لم تكن مسئولاً عن شبكة المجال، من الأفضل قبول الخيار **Standard Account** "حساب قياسي" الافتراضي.

٩. انقر الزر **Next** "التالي"، ثم انقر الزر **Finish** "إنهاء".

١٠. في مربع الحوار **System properties** "خصائص النظام"، انقر **OK** "موافق".

يبلغك مربع رسالة أنك يجب أن تعيد تشغيل كمبيوترك لكي يسري مفعول التغيير.

١١. أغلق كل الملفات والبرامج المفتوحة، ثم في مربع الرسالة، انقر الزر **Restart Now** "إعادة التشغيل الآن".

١٢. عندما يعاود كمبيوترك العمل، اضغط **Ctrl+Alt+Del** لإظهار شاشة الترحيب.

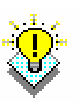
ثم اكتب أوراقك الثبوتية للمجال، واضغط مفتاح **Enter** لتسجيل الدخول إلى المجال.

الاتصال بمجال من مكان آخر

لقد كانت استراتيجيات الاتصال الهاتفي هي الطريقة الوحيدة لتأسيس اتصال عن بعد مع شبكة اتصالات خاصة (سواء كانت شبكة اتصال محلية **LAN** أو شبكة واسعة **WAN**). تزودنا الانترنت الآن باحتمال آخر للوصول عن بعد باستخدام نوع من الشبكات الذي بدأ ينتشر استخدامه في الشركات يطلق عليها **Virtual Private Network** وتختصر هكذا **VPN** ويمكن ترجمتها إلى "الشبكة الخاصة التخيلية"، تسمح هذه الشبكة لأي مستخدم في شبكة النطاق بالوصول إليها عبر شبكة الإنترنت. ومن هنا جاءت كلمة "تخيلية"، لأنك تتصل بمجالك عبر شبكة الإنترنت من بيتك أو أثناء سفرك.

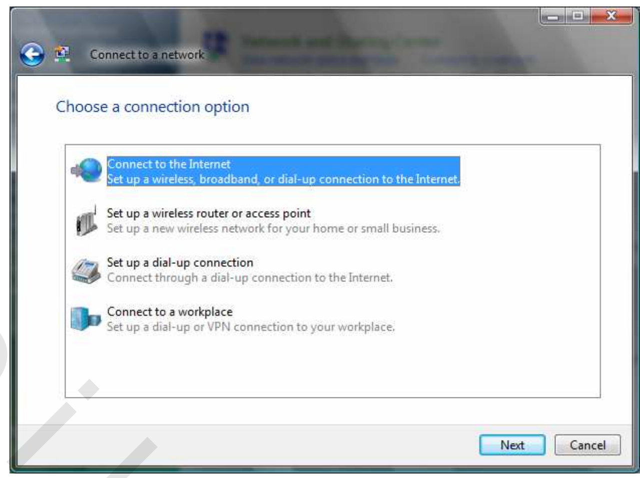
يتطلب اتصال **VPN** إلى شبكة شركتك من بعيد أن تكون شركتك قد أعدت **Server Remote Access** "خادم اتصال بعيد".

ولأنك تتصل عبر الإنترنت، فإن سرعة اتصالك **VPN** محدودة بسرعة اتصالك بالإنترنت، فالاتصال الهاتفي يكون بطيئاً جداً ويتطلب وقتاً طويلاً وصبراً لكي يصل جهازك إلى موارد الشبكة أما الاتصال عن طريق **ISDN** أو **DSL**.
فيحقق لك السرعة التي تصل إليها إذا كنت تعمل داخل النطاق.
لكي تنشئ اتصال **VPN** عبر الانترنت اتبع الآتي:



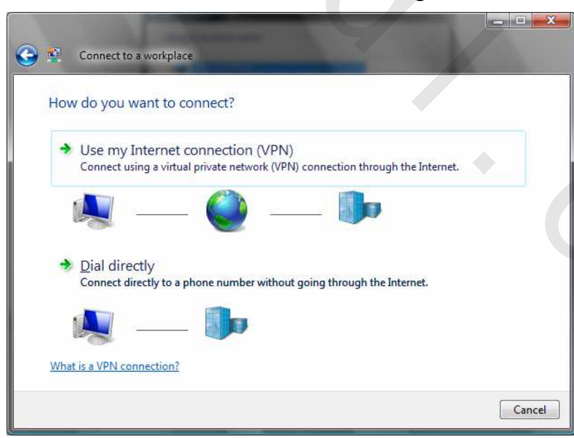
تأكد أن شركتك تملك خادم وصول بعيد **(Remote Access Server)** لكي تستطيع متابعة التمرين التالي.

١. من لوحة التحكم، انقر **Network and Internet** "الشبكة وإنترنت". يظهر الإطار **Network and Internet** "الشبكة والانترنت".
٢. تحت **Network and Sharing Center** "مركز الشبكة والمشاركة"، انقر المهمة **Connect to a Network** "الاتصال بالشبكة"، ثم في أسفل الإطار **Connect to a Network** "الاتصال بالشبكة"، انقر المهمة **Set up a connection or network** "إعداد الاتصال أو شبكة" يبدأ معالج الاتصال بالشبكة. وتظهر أول شاشة بعنوان **Choose a Connection Option** "تحديد خيارات الاتصال" (شكل ١٥-٨).



شكل ١٥–٨ تحديد خيارات الاتصال

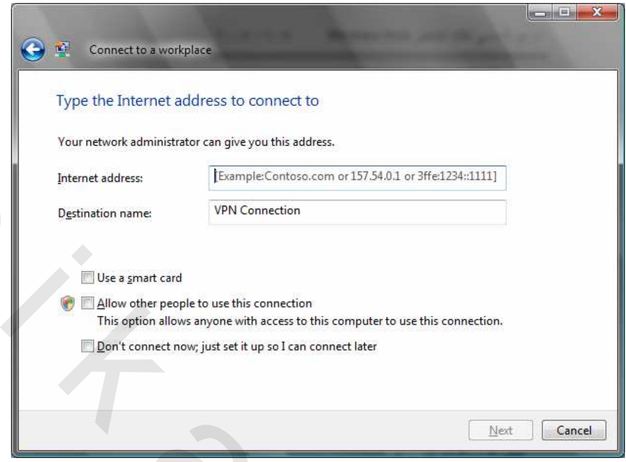
٣. استخدم شريط التمرير الرأسي للوصول إلى نهاية قائمة **Choose a connection option** "تحديد خيار الاتصال" إذا لزم الأمر للوصول إلى نهاية الخيارات المعروضة، ثم انقر **Connect to a Workplace** "اتصال بمكان العمل"، لاختياره. ثم انقر الزر **Next** "التالي". تظهر الشاشة التالية بعنوان **How do yon want to connect** "كيف تريد الاتصال" (شكل ١٥–٩).



شكل ١٥–٩ تحديد كيفية طريقة الاتصال

٤. في الصفحة **How do you want to connect** "كيف تريد إجراء الاتصال"، انقر **Use My Internet connection (VPN)** "استخدام اتصال إنترنت". تظهر

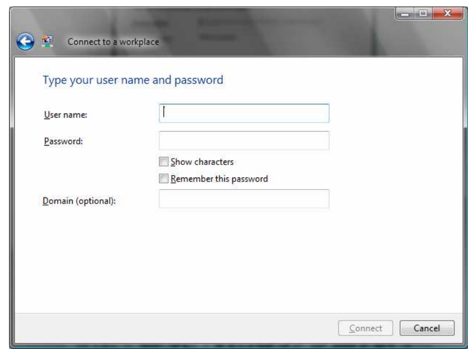
الصفحة **Type the Internet address to connect to** "اكتب عنوان إنترنت للاتصال بـــ". (شكل ١٥-١٠)



شكل ١٥-١٠ تحديد عنوان الانترنت الذي ستتصل به

٥. في المربع **Internet Address** "عنوان إنترنت"، اكتب اسم المضيف أو العنوان **IP** لخادم الوصول البعيد، وفي المربع **Destination name** "اسم الوجهة"، اكتب اسماً للاتصال (مثلاً، اسم الشركة). سيصبح زر **Next** "التالي" متاحاً (زاهياً).

٦. حدد ما إذا كنت تريد جعل الاتصال متوفراً لبقية مستخدمي كمبيوترك أو تريد الاحتفاظ به لنفسك فقط، ثم انقر الزر **Next** "التالي". تظهر الشاشة التالية تطالبك بكتابة الاسم وكلمة المرور (شكل ١٥-١١).

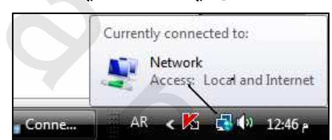


شكل ١٥-١١ مربع تحديد اسم المستخدم وكلمة المرور

٧. في الصفحة **Type your user name and password** "اكتب اسم المستخدم وكلمة المرور)، اكتب أوراقك الثبوتية على الشبكة.

لاحظ أنه يمكنك إظهار أحرف كلمة مرورك للتأكد منها قبل المتابعة. إذا نشطت هذا الخيار، ستكون كلمة مرورك مرئية في هذه الصفحة فقط، وليس خلال عملية تسجيل الدخول الفعلية.

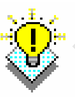
٨. انقر الزر **Connect** "اتصال". ستتصل بالشبكة. تتحقق الشبكة من اسم حسابك وكلمة مرورك، ثم تسجل دخولك. ويظهر مربع تقدم أثناء الاتصال يعلمك أن الاتصال يتم الآن. بينما يكون كمبيوترك متصلاً بالشبكة، يظهر رمز شبكة في ناحية الإعلام (شكل ١٥–١٢)، ويمكنك الاتصال بنفس موارد الشبكة التي يمكنك الاتصال بها كما لو أنك كنت تجلس في مكتبك في عملك.

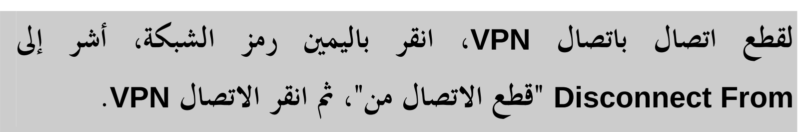


شكل ١٥–١٢ ظهور رمز الشبكة في ناحية الإعلام

٩. في معالج الاتصال بمكان العمل، انقر الزر **Close** "إغلاق". أول مرة تتصل بالشبكة، قد يطلب منك **Windows Vista** تحديد ما إذا كانت الشبكة خصوصية أو عمومية.

١٠. إذا ظهر الإطار **Set Network Location** "تعيين موقع الشبكة"، انقر **Work** "العمل". وعندما يظهر مربع الحوار **User Account Control** "التحكم في حساب المستخدم"، إذا كنت مسجلاً دخولك كمسئول، انقر الزر **Continue** "متابعة". وإلا، اكتب كلمة مرور أحد المسئولين، وانقر **OK** "موافق".





لقطع اتصال باتصال **VPN**، انقر باليمين رمز الشبكة، أشر إلى **Disconnect From** "قطع الاتصال من"، ثم انقر الاتصال **VPN**.

الوصول إلى كمبيوترك المجالي عن بعد

المقصود بـــ "الوصول إلي كمبيوترك المجالي عن بعد" الاتصال بالكمبيوتر الذي يخصك والموجود ضمن شبكة مجال من كمبيوتر آخر في موقعك البعيد كأن تكون في منزلك أو في مدينة أخري.

والميزة من هذا الاتصال البعيد بكمبيوترك الموجود في مجال أنك لن تحتاج إلي وضع كل برامجك وملفاتك في كل الأجهزة التي تعمل عليها.

يلزمك كما قلنا قبل قليل إنشاء اتصال **VPN** إلي المجال الموجود به كمبيوترك. لكي تتمكن من الاتصال بكمبيوترك الخاص، يجب أن يكون سبق ضبط تكوينه ليسمح بالوصول عبر ما يسمي **Remote Desktop** "سطح المكتب البعيد"

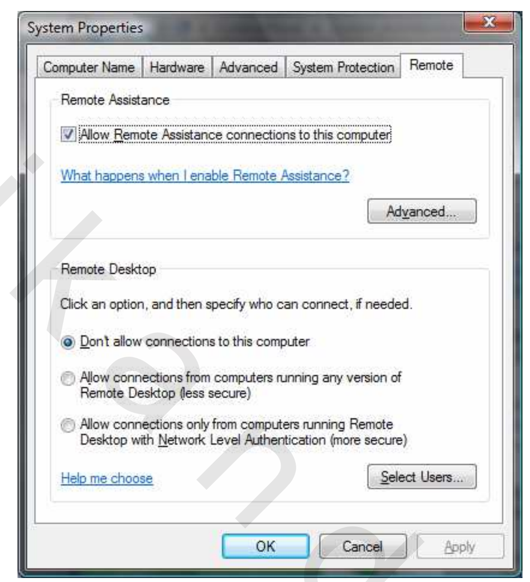
بعد الاتصال بكمبيوترك من بعيد، سيظهر سطح المكتب الذي يخص هذا الكمبيوتر علي شاشة الكمبيوتر الذي تتصل منه بكمبيوترك من بعيد. وستتمكن من العمل علي كمبيوترك من موقعك ومن الجهاز الذي تستخدمه. عندما تنهي عملك وتريد قطع الاتصال مع كمبيوترك الخاص – وهو الكمبيوتر البعيد في هذه الحالة والموجود ضمن المجال – لا توقف تشغيل كمبيوترك البعيد. بل يجب أن تسجل خروجك من الكمبيوتر البعيد عن طريق نقر زر خيارات إيقاف التشغيل في قائمة **Start** "ابدأ" ثم نقر **Log Off** "تسجيل الخروج" .

إذا أوقفت تشغيل كمبيوترك البعيد سيتم إيقافه بالفعل ولن تتمكن من الوصول إليه مرة أخري إلا إذا أعدت تشغيله أنت أو شخص آخر.

لكي تضبط كمبيوترك لتتمكن من استخدامه من خلال **Remote Desktop** "سطح المكتب البعيد" كمبيوتر آخر اتبع الآتي:

١. من لوحة التحكم، انقر **System and Maintenance** "النظام والصيانة"، ثم تحت **System** "النظام"، انقر المهمة **Allow remote access** "السماح بالوصول عن بعد". عندما يظهر مربع الحوار **User Account Control** "التحكم في حساب

المستخدم"، إذا كنت مسجلاً دخولك كمسئول، انقر الزر **Continue** "متابعة"، وإلا، اكتب كلمة مرور أحد المسئولين، وانقر **OK** "موافق". يظهر مربع الحوار **System Properties** "خصائص النظام"، عارضاً علامة التبويب **Remote** "بعيد". (شكل ١٥-١٣)

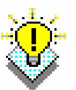


شكل ١٥-١٣ التبويب **Remote** في مربع الحوار **System Properties**

٢. تحت **Remote Desktop** "سطح المكتب البعيد"، نشط مربع الاختيار **Allow Connections from computers running any version of Remote Desktop** "السماح باتصالات من أجهزة تستخدم أي إصدار من سطح المكتب البعيد" للسماح بحصول اتصالات "سطح المكتب البعيد" من أي كمبيوتر آخر يعمل بنظام **Windows**، لحصر الاتصالات بالكمبيوترات التي تشغل **Windows Vista**، نشط مربع الاختيار **Allow connections only from computers running remote Desktop with Network Level Authentication** "السماح فقط باتصالات من أجهزة كمبيوتر تشغل سطح المكتب البعيد باستخدام مصادقة مستوى الشبكة".

٣. إذا كان كمبيوترك معداً لينام بعد فترة محددة من عدم الاستعمال، تنصحك رسالة من

"سطح المكتب البعيد" بأنك لن تكون قادراً على الاتصال من خلال "سطح المكتب البعيد" عندما يكون الكمبيوتر في صيغة النوم. انقر **OK** "موافق" لإغلاق مربع الرسالة.

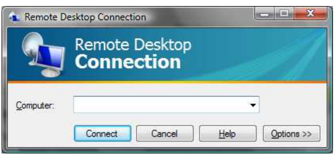


أي مسئول في كمبيوترك يكون مسموحاً له بشكل افتراضي كمستخدم بعيد. إذا كنت تريد ترخيص مستخدمين بعيدين إضافيين، أنقر الزر **Select Users** "تحديد المستخدمين"، ثم في مربع الحوار **Remote Desktop Users** "مستخدمو سطح المكتب البعيد"، انقر الزر **Add** "إضافة". يمكنك إضافة مستخدمين فرديين أو مجموعات من المستخدمين.

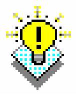
٤. في مربع الحوار **System properties** "خصائص النظام"، انقر **OK** "موافق". لكي تتصل بكمبيوترك الذي تم ضبطه من خلال سطح المكتب البعيد من كمبيوتر آخر تابع الخطوات الآتية:

٥. من كمبيوتر آخر على المجال، في القائمة **Start** "ابدأ"، أشر إلى **All Programs** "كافة البرامج"، انقر **Accessories** "البرامج الملحقة"، ثم انقر **Remote Desktop Connection** "الاتصال بسطح المكتب البعيد". يظهر الإطار **Remote Desktop Connection** "اتصال سطح المكتب البعيد".

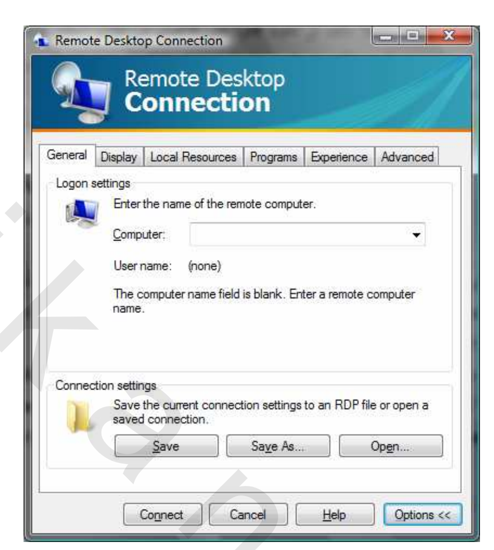
٦. إذا كانت نافذة **Remote Desktop Connection** "اتصال بسطح المكتب البعيد" لا تعرض علامات التبويب كما في شكل ١٥-١٤، انقر الزر **Options** "خيارات" لتظهر علامات التبويب المتعددة كما في شكل ١٥-١٥.



شكل ١٥-١٤ مربع الحوار **Remote Desktop Connection** "اتصال بسطح المكتب البعيد"

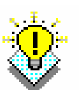


يمكنك التحكم بتوفر موارد كمبيوترك خلال جلسة عمل عن بعد بتنشيط الخيارات في علامة التبويب **Local Resources** "الموارد المحلية".



شكل ١٥-١٥ تبويبات مربع **Remote Desktop Connection**

٧. في المربع **Computer** "الكمبيوتر"، اكتب اسم الكمبيوتر البعيد الذي تريد الوصول إليه، ثم انقر الزر **Connect** "اتصال".



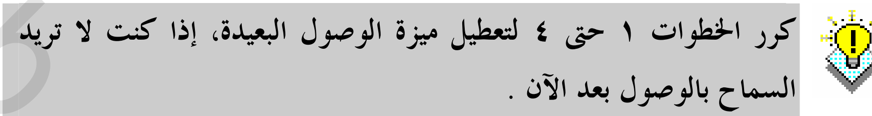
إذا كنت لا تعرف اسم الكمبيوتر، يمكنك نقر سهم المربع **Computer** "الكمبيوتر"، نقر **Browse for More** "استعراض المزيد" في القائمة التي تظهر، ثم ابحث عن الكمبيوتر الذي تريد الاتصال به في مربع الحوار **Browse for Computers** "استعراض أجهزة الكمبيوتر"، ثم انقر **OK** "موافق".

يظهر مربع الحوار **Windows Security** "أمان ويندوز".

٨. اكتب اسم المستخدم وكلمة المرور الخاصة بكمبيوترك أو مجالك. إذا كنت ستتصل بالكمبيوتر البعيد من هذا الكمبيوتر بشكل دوري، نشط مربع الاختيار

Remember My credentials "تذكر بيانات الاعتماد". ثم انقر OK "موافق".
يظهر إطار جديد على شاشتك، عارضاً سطح مكتب الكمبيوتر البعيد.

٩. استكشف الكمبيوتر البعيد، ثم عندما تصبح جاهزاً، سجل الخروج منه.


كرر الخطوات ١ حتى ٤ لتعطيل ميزة الوصول البعيدة، إذا كنت لا تريد السماح بالوصول بعد الآن .

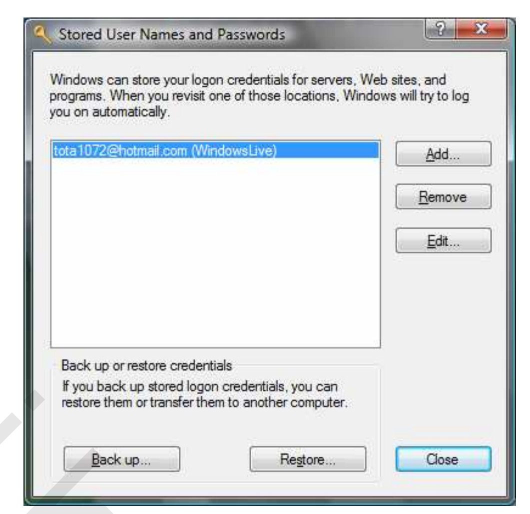
تخزين وإدارة كلمات مرور الشبكة

عندما تتصل من بعد بمجال، يتولى Windows Vista تلقائيا تخزين اسمك وكلمة المرور على الكمبيوتر الذى تستخدمه. تسمى بياناتك (اسمك وكلمة مرورك) credentials "أوراق ثبوتية". لكن ربما تغيير فى أوراقك الثبوتية هذه أثناء العمل على كمبيوترك. مثلا تغير كلمة المرور لانكشافها. إذا حدث ذلك فإن Windows يحتفظ بهذه البيانات الجديدة "الأوراق الثبوتية" ويمررها تلقائيا الى المجال عندما تتصل به فى المرة القادمة.

لتخزين كلمة مرور شبكة اتبع الآتي:

١. من لوحة التحكم، انقر User Accounts and Family Safety "حسابات المستخدمين وأمان العائلة"، ثم انقر User Accounts "حسابات المستخدمين".

٢. في قائمة Tasks "المهام"، انقر Manage your network passwords "إدارة كلمات المرور للشبكة". يظهر مربع حوار Stored user names and Passwords "أسماء مستخدمين وكلمات مرور مخزنة". شكل ١٥-١٦



شكل ١٥-١٦ مربع **Stored User Names and Passwords**

٣. من مربع الحوار **Stored user names and Passwords** "أسماء مستخدمين وكلمات مرور مخزنة"، انقر الزر **Add** "إضافة".

يظهر مربع الحوار **Stored Credential Properties** "خصائص بيانات الاعتماد المخزنة".

٤. في المربع **Log on to** "تسجيل الدخول إلى"، اكتب الخادم أو موقع الويب أو البرنامج الذي تريد تخزين الأوراق الثبوتية له.

٥. في المربعات **User name** "اسم المستخدم" و **Password** "كلمة المرور"، اكتب أوراقك الثبوتية للخادم أو لموقع الويب.

٦. تحت **Credential** "نوع بيانات الاعتماد"، نشط نوع الكيان الذي تخزن الأوراق الثبوتية له. ثم انقر **OK** "موافق"

ملخص الفصل

شرحنا في هذا الفصل أكثر من طريقة للاتصال بالشبكات وبدأنا بشرح كيفية وصل جهازك بمجموعة عمل جديدة ثم شرحنا خطوات توصيل كمبيوترك بشبكة نطاق أو مجال وتعرضنا لكيفية الاتصال بمجال من مكان لآخر وأخيراً شرحنا كيفية الوصول إلي

كمبيوترك المجالي عن بعد .

تدريبات

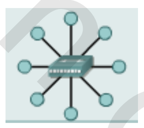
١. اتبع خطوات توصيل جهازك بكل من :

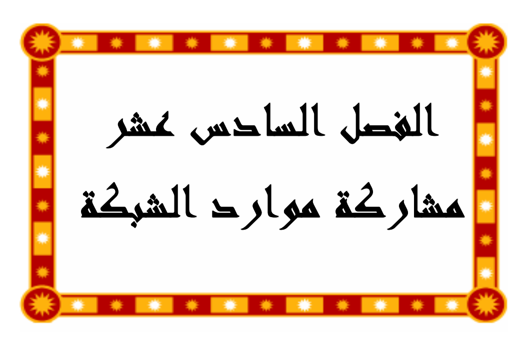
أ. مجموعة عمل.

ب. شبكة نطاق.

ج. مجال في مكان بعيد.

ثم أطلع مدربك علي نتيجة عملك.





الموارد هي مشغلات الأقراص والمجلدات والملفات والطابعـــات المشتركة. ولعل مشاركة موارد الشبكة هي أهم هدف يـــسعي إليه مستخدموا الشبكات. بانتهاء هذا الفصل ستتعرف علي :

- *مفاهيم ضرورية قبل الحديث عن مشاركة الموارد.*
- *تسمية ملفات المشاركة الموجودة علي الشبكة.*
- *الشبكة ومركز المشاركة.*
- *استكشاف الشبكة والبحث عن الموارد.*
- *تخصيص صلاحيات المشاركة والتعامل معها.*
- *مشاركة مشغل الأقراص.*
- *مشاركة المجلدات والملفات.*
- *مشاركة الطابعات وتحديد صلاحياتها.*

قبل أن نتحدث عن مشاركة محركات الأقراص والمجلدات نوضح بعض المفاهيم الضرورية والتي ستحتاجها أثناء تعاملك مع شبكة اتصالات **Windows Vista**.

***المجال* Domain**

هو تجميع منطقي (بدلا من مادي) لموارد الشبكة (وهي أجهزة الخادم ومحطات العمل وباقي الأجهزة الأخرى. تدار الشبكة التي تستخدم الميدان بواسطة **Windows 200x Server (Windows 2000/2003/2008Server)**. مستخدمي المجال معروفين لكل جهاز على الشبكة، ولذلك فإن الشخص الذي يسجل دخوله إلى الميدان بواسطة حساب مستخدم، يستطيع أن يصل إلى موارد الميدان من أي كمبيوتر يعمل عليه.

عندما تحدد أنت أو مدير الشبكة من يحق له صلاحيات الوصول إلى الملفات ومن لا يحق له ذلك، يمكنك اختيار المستخدمين والمجموعات من قائمة جميع المستفيدين الموجودين بشركتك. ويمكنك منح صلاحيات لأشخاص معينين، أو لإدارات معينة أو لمواقع محددة.

مجموعة العمل Workgroup

هي مجموعة منطقية من أجهزة الكمبيوتر لا تدار مركزياً وإنما تتصل ببعضها من خلال شبكة. هذا معناه أن كل جهاز كمبيوتر في مجموعة العمل له قائمة منفصلة خاصة به موجود بها أسماء المستفيدين (المستخدمين). ولا يسجل المستخدمون الفرديون دخولهم إلى مجموعة العمل. هذا الأمر يجعل من الصعب أن تتأكد من أن مستخدما لأحد الأجهزة له صلاحيات الوصول إلى جهاز آخر أم لا.

قدمت **Windows Vista** دعم هائل لإنشاء الشبكة والتعامل معها ، كما قدمت دعـــم هائل لمشاركة الملفات والمجلدات **Sharing Folders** بحيث تستطيع التعامل مع ملفات ومجلدات المشاركة الموجودة علي أي جهاز من أجهزة الشبكة كما لو كان هذا المجلد علي جهازك المحلي. ولم يتبقي لمستخدمي الشبكة من خلال **Windows Vista** سوي البحث عن الموارد **Resources** وتحديدها.

(وعندما نتكلم عن الموارد هنا نقصد ملفات أو مجلدات المشاركة الموجودة علي الشبكة أو

الطابعات المعرفة علي الشبكة أو حتي مواقع المشاركة).

تستطيع مشاركة الملفات والمجلدات في **Windows Vista** بطريقتين :

- الطريقة الأولي : بنفس مفهوم المشاركة الموجود في الإصدارات السابقة من **Windows** وهو عن طريق اختيار الملف أو المجلد ثم ضبط خاصية المشاركة له وهي تظهر في القائمة التي تظهر عند النقر علي المجلد بالزر الأيمن للماوس.
- الطريقة الثانية : وهي الطريقة الجديدة التي تدعمها **Windows Vista** هي وضع الملف أو المجلد الذي ترغب في مشاركته في المجلد العمومي **Public Folder** الموجود في **Windows Vista** بحيث يستطيع أي مستخدم للشبكة رؤية هذه الملفات/المجلدات والتعامل معها بناء علي الصلاحيات الممنوحة له.

لكي تجعل مشاركة الملفات على الشبكة متاحة ومفهومة لمستخدمي الشبكة يجب أن تستخدم إحدى طريقتين

❖ الأولي : إذا أردت أن تجعل مشاركة الملفات متاحة لجميع مستخدمي الشبكة، ولا تريد أن تصنع قيوداً على من يستخدم الملفات والمجلدات المشتركة عطل إمكانية **Password Protected Sharing** على جميع أجهزة الكمبيوتر واسمح لأي مستخدم أن يضع الملفات التي يرغب في مشاركتها على المجلد **Public** على جهازه.

بهذه الطريقة يستطيع أي مستخدم تسجيل دخوله من أي جهاز كمبيوتر والتعامل مع الملفات المشتركة. والعيب في هذه الطريقة، أن أي شخص يستطيع الاتصال بالشبكة والوصول إلى الملفات حتى ولو كان مسجلا دخوله كحساب ضيف **(Guest)**.

❖ الثانية : أما إذا أردت أن تحمي الملفات والمجلدات المشتركة الموجودة على الشبكة، بحيث تحدد من هو المستخدم الذي له صلاحيات الوصول إلى الملفات المشتركة، يجب أن تجعل إمكانية **Password Protected Sharing** متاحة على كل جهاز كمبيوتر ترغب في مشاركة ملفاته. وأن تنشئ نفس مجموعة حسابات المستخدمين على جميع الأجهزة مع تخصيص نفس الاسم وكلمة المرور لكل مستخدم.

هذه الطريقة آمنة، لكن يكتنفها بعض الصعوبات تتمثل في عملية تخصيص الأسماء وكلمات المرور على جميع الأجهزة. أيضا إذا قام أحد المستخدمين بتغيير كلمة مروره على أحد الأجهزة، فلابد من تغيير نفس الكلمة على باقي الأجهزة.

تسمية ملفات المشاركة الموجودة علي الشبكة

بواسطة الأذونات الملائمة، يستطيع المستخدم الميداني الاتصال بكمبيوتر مستخدم ميداني آخر، بواسطة كتابة العنوان **UNC** الخاص بذلك الكمبيوتر (سنعود لشرح تسمية **UNC** بعد قليل) هذا معناه أن الوصول إلي ملفات ومجلدات المشاركة يتم بواسطة اصطلاح التسمية العالمي **UNC** (اختصاراً لعبارة **Universal Naming Convention**) مع **Windows Vista** كما كان في الإصدارات السابقة من **Windows**. وستلاحظ أن الفرق بين تسمية الملفات المحلية والملفات الموجودة علي الشبكة هو فقط في التسمية. عندما نجد أن اسم الملف يبدأ بشرطتين مائلتين هكذا :\\ تعرف أن هذا الملف ملف مشارك (**Shared File**) موجود علي الشبكة. وفيما يلي نوضح كيفية تسمية الملفات ومجلدات المشاركة (**Sharing Files and Folders**) الموجودة علي الشبكة.

يخصص لكل جهاز كمبيوتر موجود علي شبكة محلية **LAN** أو شبكة انترانت (**Intranet**) أو حتي شبكة انترنت عالمية **Internet** اسم مميز لا يشترك فيه غيره من الأجهزة الموجودة علي الشبكة. كما أن كل مجلد أو طابعة مشتركة موجودة علي الشبكة لها أيضا اسم مميز.

تجعل المشاركة أو **Sharing** المجلد أو حتى القرص الصلب بكامله متاحاً للآخرين على الشبكة. فمثلاً إذا كان مخصص لجهازي كمبيوتر على الشبكة الاسم **Magdy** وكان المجلد المشارك الموجود على الشبكة باسم **C:\Documents** فإن جميع مستخدمي الشبكة يستطيعون استخدام هذا الملف بالاسم الشبكي المخصص له وهو:

\\magdy\docs

ولعلك تتساءل: لماذا اختلف اسم المجلد الموجود على القرص الصلب وهو **C:\documents** عن الاسم الشبكي في حالة المشاركة وهو: **docs**

السبب أن أسماء المجلدات المشتركة الموجودة على الشبكة يجب ألا تزيد عن ١٢ حرفاً وألا

تشتمل على فراغات. وهذا بخلاف ما تعلمه وما تستخدمه مع نسخة ملفات ومجلدات **windows Vista** المحلية التي يسمح فيها بفراغات وأن يكون اسم الملف / المجلد طويلاً جدا. أرجو ألا يسبب لك هذا الأمر أي نوع من الإرباك عن نسخة الملفات المشاركة على الشبكة.

والآن نعود إلى شرح المصطلح **UNC** الذي وعدناك بالعودة لتوضيحه.

UNC اختصار للعبارة **Universal Naming Convention** ويمكن ترجمتها "اصطلاح التسمية العالمي"، وهو مفهوم أو اصطلاح في تسمية الملفات المشاركة على الشبكة يستخدمه المستخدم الموجود على جهاز كمبيوتر آخر للإشارة إلى اسم الملف/المجلد الذي يرغب في مشاركته.

وللتوضيح أقول عادة أقوم بالتعرف على الملف الموجود على القرص المغناطيسي الخاص بي عن طريق اسم الملف والمسار **(Path)** الموصل لهذا الملف هكذا

C:\documents\budget 2008.xlsx

أما المستخدم الموجود على جهاز كمبيوتر آخر فإنه يشير إلى هذا الاسم عن طريق ما يسمى **UNC** هكذا.

\\magdy\Docs\budget 2008.xlsx

توضح **** أن **magdy** هو اسم جهاز الكمبيوتر الموجود على الشبكة بدلا من اسم الدليل الموجود في الدليل الجذري للقرص الصلب.

أما **Docs** فهو اسم ملف المشاركة الموجود تحت الدليل الجذري، وكل ما يتبعه يحدد المسار والملف المنسوب لهذا المجلد المشارك.

إذا كان الكمبيوتر الذي تريد استخدام ملفاته على الشبكة يستخدم الدليل النشط **(Active Directory)** أو كان جزءا من شبكة بعيدة. بإمكانك تسمية الكمبيوتر البعيد بالاسم الكامل هكذا:

\\magdy.Compuscience.Com\docs\budget 2008.xlsx

أما إذا كنت تعرف عنوان **IP** الخاص بهذا الكمبيوتر (مثلاً إذا كنت تتصل بالكمبيوتر البعيد عن طريق اتصال هاتفي). يمكنك استخدام عنوان **IP** هكذا

\\192.168.0.10\docs\budget 2008. xlsx

الطابعات المشتركة يخصص لها أيضا اسم مشترك ويتم تعريفها بمسار **UNC** الخــاص بهــا. فمثلاً لو أردت مشاركة طابعة **HP**، وكنت خصصت لها الاسم المشترك **HPLaser** سيتم الوصول إليها من الشبكة هكذا:

//magdy/HPLaser

رغم أنها ليست مجلدا وإنما طابعة، إلا أن **Windows** سيتعرف على المــصادر المختلفــة للشبكة.

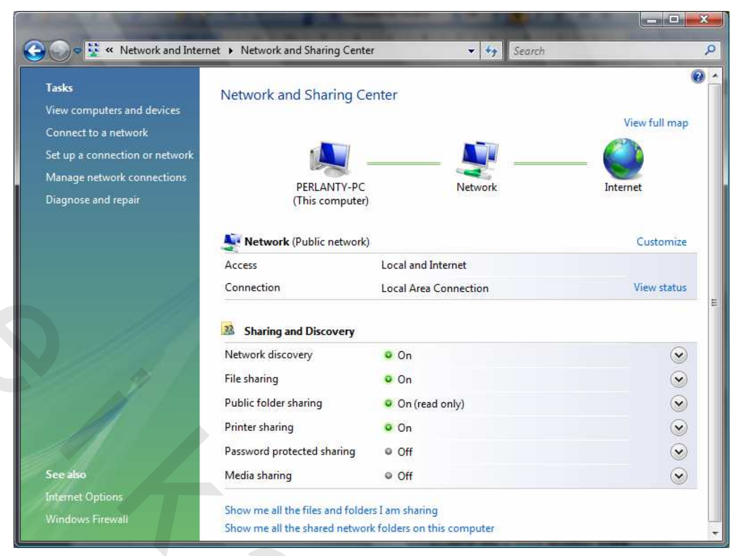
الشبكة ومركز المشاركة

مركز الشبكة والمشاركة **Network and Sharing** في **Windows Vista** هو المركز الرئيسي للعمل مع إعدادات الشبكة فمن خلاله تستطيع أن تري الخــصائص المختلفــة كحالة الشبكة وتفاصيلها وملخصات عن حالة أجهزة الكمبيوتر المتصلة بالشبكة....الخ.

لفتح مركز الشبكة والمشاركة تابع الخطوات التالية:

١. افتح قائمة **Start** "ابدأ" ثم اختر **Control Panel** "لوحة التحكم" .

٢. من نافذة **Control Panel** "لوحة التحكم" انقــر الارتبــاط **Network and Internet** "الشبكة والانترنت" ومن النافذة التي ستظهر أمامك اختر **Network and Sharing Center** "مركز الشبكة والمشاركة" ستظهر أمامك نافذة مركــز الشبكة والمشاركة. شكل ١٦–١



شكل ١٦-١ مركز الشبكة والمشاركة في **Windows Vista**

تحتوي نافذة مركز الشبكة والمشاركة علي ثلاث مناطق مهمة هي :

Network Map "الشبكة" : وهي توضح رسم تخطيطي بسيط يوضح مواقع أجهزة الكمبيوتر في الشبكة وإذا كانت متصلة بالانترنت .

Status "عرض الحالة" : تعطيك تفاصيل إضافية عن تكوين الشبكة الحالي.

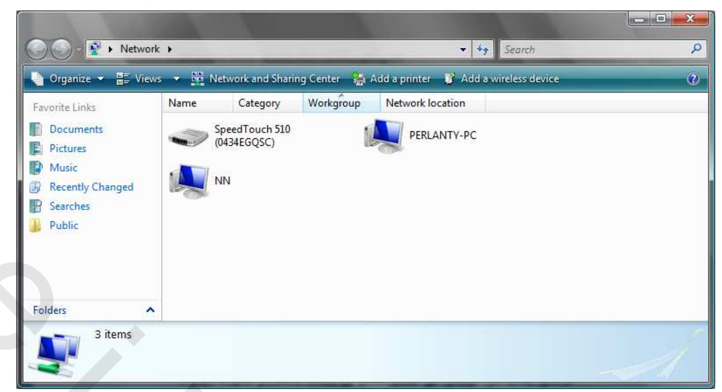
Sharing and Discovery مشاركة واكتشاف" : تزودك بمعلومات إضافية عن الإعدادات الخاصة بالمشاركة واكتشاف الشبكة.

البحث عن موارد المشاركة في الشبكة

تحدثنا سابقاً أنك لكي تستفيد من الشبكة، يجب أن تعرف الموارد والعناصر المتاح لك التعامل معها علي الشبكة وتبادل البيانات بينك وبين باقي المستخدمين من خلالها.

إذا كنت قد اعتدت علي العمل مع أنظمة **Windows** السابقة فستعرف أن العمل الواحد يمكن تأديته بأكثر من طريقة ولعل أكثر الطرق المباشرة للتعرف علي العناصر الموجودة علي الشبكة من طابعات ومجلدات ومواقع مشاركة هي استخدام **Network Explorer** "مستكشف الشبكة" . لفتح مستكشف الشبكة انقر **Start** "ابدأ" ومن

القائمة اختر **Network** "الشبكة".ستظهر نافذة المستكشف كما في شكل ١٦-٢



شكل ١٦-٢ نافذة مستكشف الشبكة يعرض رموز الأجهزة الموصلة علي الشبكة

يظهر في نافذة المستكشف اختصارات لجميع مصادر الشبكة المألوفة مثل المجلدات المشتركة ومجلدات الويب.

عندما تقوم بإعداد **Windows** لن يظهر في نافذة المستكشف أي من اختصاراتك الشخصية، أما إذا قمت بإعداد **Windows** علي شبكة مجموعة عمل **Workgroup** **Network** سيظهر اختصار أو رمز لكل جهاز كمبيوتر في مجموعة العمل هذه في نافذة المستكشف.

أما في حالة الشبكة من نوع **Domain** "المجال" فيجب أن تعرض مصادر الشبكة من خلال الشبكة أو أن تطلب من مدير الشبكة أن يعرف لك المجلدات المشتركة. سنشرح بعد قليل كيف تستعرض مصادر الشبكة.

كما تحتوي نافذة المستكشف علي العديد من المهام التي يمكنك القيام بها من هذه المهام ما يلي :

- **Add Printer** "إضافة طابعة" : لفتح معالج لإضافة الطابعة سواء إضافتها كطابعة محلية أو طابعة مشاركة علي الشبكة .
- **Add Wireless Device** "إضافة جهاز لاسلكي" : لفتح المعالج المسئول عن إضافة جهاز لاسلكي إلي الشبكة مثل كارت الشبكة اللاسلكي مثلاً .

- View Computers and Devices "عرض الأجهزة والمكونـات": لعـرض أجهزة الكمبيوتر والأجهزة التي يراها جهازك ويتعامل معها .
- Connect to Network "الاتصال بالشبكة": لكي يربط جهازك بجهاز آخـر أو بالشبكة.
- Setup a Connection or Network "إعداد الاتصال بالشبكة" : لبدء المعالج المسئول عن ربط جهازك بأنواع أخري من الشبكات.
- Mange Network Connections "إدارة اتصالات الشبكة" : لفـتح نافـذة أخري توضح المكونات المادية في الشبكة ككارت الشبكة وغير ذلك من الأجهزة.
- Diagnose and Repair "التشخيص والإصلاح" : لحـث Windows علـي إيجاد حلول للمشكلات والعيوب الشائعة التي قد توجد في الشبكة .

استكشاف الشبكة والبحث عن الموارد

تحدثنا سابقاً أنك تستطيع التعامل مع الموارد المختلفة علي الشبكة (والموارد هي الملفـات والمجلدات والطابعات المشتركة) وللتعامل مع هذه الموارد يجب عليك أولاً البحث عنـها والوصول إليها كي تستطيع التعامل معها، وكذلك التعرف علي الخصائص المختلفة لتلك الموارد. كما أشرنا أن مستكشف الشبكة Network Explorer يقوم بعرض المـوارد الموجودة علي الشبكة وهو يعمل بـنفس مفهـوم مستكـشف وينـدوز Windows Explorer ويستطيع البحث عن موارد الشبكة المختلفة وعرضها.

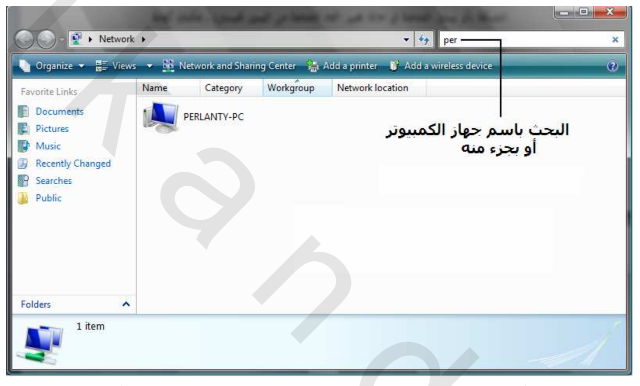
في الشبكة من نوع مجموعة العمل Workgroup Network، يظهر تلقائياً رمز لكـل جهاز من أجهزة الشبكة. عندما تقوم بتوسيع هذه الرموز (أو بفتح رمز الكمبيوتر) يمكن استخدام المجلدات والطابعات المشتركة الموجودة عليها بنفس الطريقة التي تـستخدم بهـا المجلدات الموجودة على قرصك الصلب.

إما إذا كنت تستخدم شبكة من نوع Domain "المجـال" تـستخدم الـدليل النـشط، Active Directory، ستظهر رموز إضافية للبحث في الدليل النشط.

وفيما يلي نوضح كيف يمكن البحث في الشبكة عن الأجهزة، والمجلدات والملفات.

البحث عن أجهزة الكمبيوتر المتصلة بالشبكة

من نافذة مستكشف الشبكة **Network Explorer** (راجع شكل ١٦-٢) تستطيع البحث عن أجهزة الكمبيوتر المتصلة بالشبكة عن طريق استخدام مربع البحث الموجود في أعلي يمين الشبكة (أو يسار الشاشة في حالة تغيير اتجاه الشاشة من اليمين لليسار) ، يمكنك كتابة اسم الكمبيوتر الذي تبحث عنه أو كتابة جزء فقط من الاسم وسيقوم مستكشف الشبكة بالبحث عن هذا الجهاز وعرضه . شكل ١٦-٣



شكل ١٦-٣ البحث عن جهاز كمبيوتر في الشبكة

البحث عن الملفات والمجلدات الموجودة علي أي جهاز في الشبكة

يمكنك استخدام نفس مفهوم البحث عن الملفات والمجلدات علي جهازك المحلي للبحث عن الملفات والمجلدات الموجودة علي الشبكة.

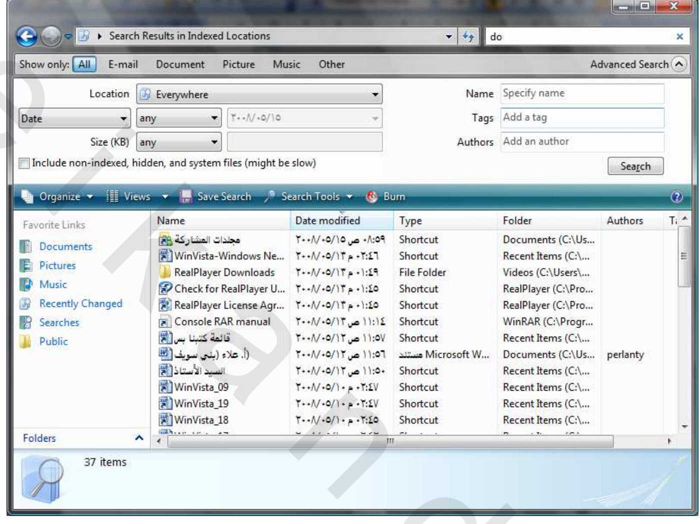
للبحث عن الملفات سواء علي جهازك أو علي مجلدات المشاركة علي الشبكة تابع الخطوات التالية :

١. افتح قائمة **Start** "ابدأ" ثم اختر الأمر **Search** "بحث"، سيظهر المربع الحواري **Search** "بحث" ويظهر في أعلاه مربع البحث الذي تكتب فيه اسم الملف أو النص الذي تبحث عنه.

٢. انقر **Advanced Search** "بحث متقدم" أعلي المربع الحواري، ستظهر خانات

البحث الخاصة بالبحث المتقدم .

٣. من خانة Location "الموقع" اختـــر Everywhere "في كـــل مكـــان" ليقـــوم Windows بالبحث عن الملف المطلوب في جهازك المحلي أو في أي جهـــاز مـــن أجهزة الشبكة. شكل ١٦-٤.



شكل ١٦-٤ البحث عن الملف سواء علي الجهاز المحلي أو أجهزة الشبكة

٤. إذا عثر Windows علي الملف الذي تبحث عنه يظهره في نتيجة البحث ويظهـــر مكانه سواء كان علي جهازك المحلي أو أي جهاز من أجهزة الـــشبكة أو أي مجلـــد مشاركة.

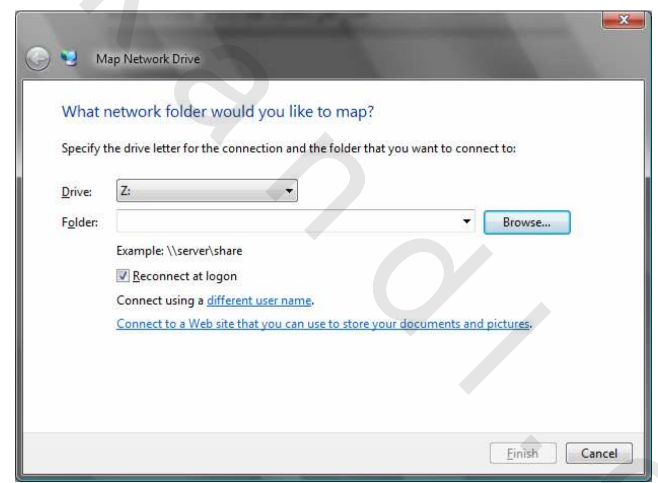
تخصيص اسم لمجلدات أو أجهزة المشاركة Mapping Drive Letters

إذا كنت كثيراً ما تستخدم جهاز أو مجلد المشاركة الموجود علي الـــشبكة ، فيمكنـــك تخصيص اسم (أو حرف) لهذا الجهاز/المجلد المشترك بحيث يظهر وكأنه جزء من القـــرص الصلب المحلي الخاص بجهازك كالجزء C:\ أو D:\ مثلاً. ويكون هذا الحرف الذي يخصص لجهاز/مجلد المشاركة يلي ترتيب الحروف المتتالية المخصصة لأجـــزاء القـــرص الـــصلب الموجود في جهازك، وكذلك مشغل الأقراص المدمجة CD-Rom (فإذا كانت الحـــروف

المخصصة لأجزاء قرصك الصلب ومشغل الأقراص المدمجة **CD-Rom** تنتهي عند الحرف **F** مثلاً، فيمكنك تخصيص الحرف **I** لجهاز/مجلد المشاركة الموجود علي الشبكة ، قد تفيدك عملية تخصيص حرف لجهاز/مجلد المشاركة في تسهيل التعامل مع جهاز/مجلد المشاركة وتزيد سرعة التعامل مع الملفات المخزنة عليه واستعراضها.

لتخصيص حرف لجهاز/مجلد المشاركة اتبع الخطوات التالية:

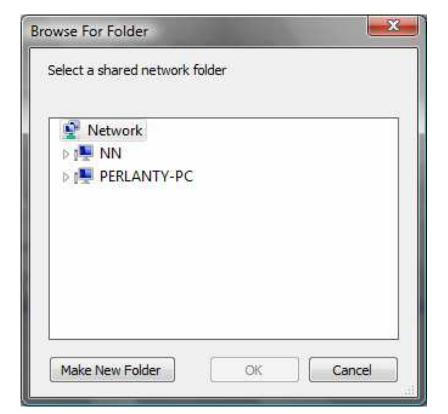
١. من قائمة **Start** "ابدأ" انقر الأمر **Network** "الشبكة" بزر الفأرة الأيمن ومن القائمة المختصرة اختر الأمر **Map Network Drive** "تعيين محرك أقراص الشبكة" ، سيظهر المربع الحواري **Map Network Drive** "تعين محرك أقراص الشبكة" . شكل ١٦-٥.



شكل ١٦-٥ المربع الحواري **Map Network Drive** "تعيين محرك أقراص الشبكة"

٢. قم باختيار الحرف الذي تريد تخصيصه لجهاز/مجلد المشاركة .

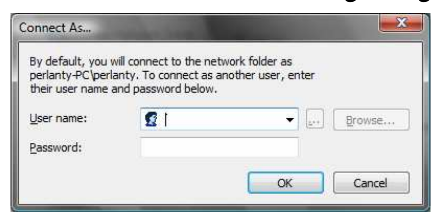
٣. لتحديد اسم أو مكان جهاز/مجلد المشاركة الذي تريد تخصيصه انقر زر **Browse** "استعراض" سيظهر المربع الحواري **Browse For Folder** "الاستعراض بحثاً عن مجلد" . شكل ١٦-٦ لتختار منه الجهاز أو المجلد الذي تريد تخصيص الاسم له ، بعد تحديد الجهاز أو مجلد المشاركة الموجود علي أي جهاز من أجهزة الشبكة ، انقر **OK** "موافق".



شكل ١٦–٦ مربع تحديد جهاز/مجلد المشاركة

٤. سيغلق المربع الحواري وتعود للمربع الحواري **Map Network Drive** "تعيين حرف محرك أقراص شبكة" ومن هذا المربع أمامك اختيارين :

- إذا كنت تريد أن يظهر هذا التخصيص في كل مرة تستخدم فيها الجهاز، قم بتحديد خانة الاختيار **Reconnect at Logon** "إعادة الاتصال عند تسجيل الدخول" . فإذا لم تقم بتحديد هذا الاختيار سيختفي هذا التخصيص بمجرد خروجك **Log off**.
- إذا كانت صلاحياتك الحالية غير كافية للتعامل مع الأجهزة/المجلدات المشتركة ، انقر الارتباط **Connect Using Different Username** "الاتصال باستخدام اسم مستخدم مختلف" ، سيظهر مربع حواري آخر لإدخال اسم مستخدم بديل. شكل ١٦–٧



شكل ١٦–٧ مربع إدخال اسم المستخدم البديل

٥. بعد الانتهاء من تخصيص جهاز/مجلد المشاركة انقر زر **Finish** "إنهاء"، سيختفي المربع

الحواري ويظهر الجهاز/المجلد أمام في نافذة Computer "الكمبيوتر" كأنه جزء من قرصك الصلب ولكن بشكل مختلف قليلاً . شكل ١٦-٨



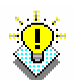
شكل ١٦-٨ ظهور مجلد المشاركة في نافذة Computer "الكمبيوتر"

مشاركة المجلدات

تتيح لك Vista Windows طريقتين أساسيتين لمشاركة الملفات إما عن طريق استخدام المجلدات العامة Folders Public الموجود في Windows أصلاً أو باستخدام طرق المشاركة التقليدية المعروفة للمجلدات ، يحتوي مركز الشبكة والمشاركة الذي تحدثنا عنه سابقاً علي المكان الرئيسي الذي تستطيع من خلاله إدارة مشاركة الملفات في Windows Vista ولكن تعتمد طريقة مشاركة المجلدات والملفات علي نوع الشبكة التي تستخدمها كما أشرنا سابقاً .

مشاركة المجلدات للشبكات من نوع مجموعة العمل Workgroup

في الشبكات من نوع مجموعات العمل وفرت Microsoft دعماً للتعامل وتأمين مشاركة الملفات عن طريق مجلد Folder Public "مجلد عمومي" مع إمكانية حماية المشاركة بكلمات مرور للمستخدمين ، إذا كانت شبكتك من هذا النوع تابع الشرح التالي.



عندما تشارك المجلدات علي جهاز يستخدم المجلد العام **Public Folder** في الوضع **Enabled** "تمكين"، يستطيع أي مستخدم للجهاز الاطلاع علي الملفات والتعديل فيها إذا أعطيت صلاحيات التعديل في المجلد العام **Public Folder**.

لكي يؤدي المجلد العام **Public folder** وظيفته يجب أن يكون مُمكن **Enabled** ، وتستطيع تمكينه من نافذة **Network and Sharing Center** "مركز الشبكة والمشاركة" بإتباع الخطوات التالية:

١. افتح قائمة **Start** "ابدأ" ثم اختر **Control Panel** "لوحة التحكم" .
٢. من نافذة **Control Panel** "لوحة التحكم" انقر الارتباط **Network and Internet** "الشبكة والانترنت" ومن النافذة التي ستظهر أمامك اختر **Network and Sharing Center** "مركز الشبكة والمشاركة" ستظهر أمامك نافذة مركز الشبكة والمشاركة. (راجع شكل ١٦-١)
٣. من الجزء **Sharing and Discovery** "المشاركة والاكتشاف" الموجود في منتصف النافذة ، انقر السهم ⌄ الموجود بجوار الاختيار **Public Folder Sharing** "مشاركة مجلد عام" سيتمدد هذا الجزء ليظهر الخيارات المختلفة التي سيتعامل بها المستخدمون مع هذا المجلد، فيمكنك تمكين (تشغيل) هذا المجلد العام أو إيقاف تمكينه كما يمكنك تحديد إذا كان مسموح للمستخدمين التعديل فيه أم لا.

بعد تمكين المجلد العام **Public Folder** من العمل يمكنك مشاركة الملفات والمجلدات من خلاله لعمل ذلك تابع الخطوات التالية :

١. افتح نافذة مستكشف ويندوز **Windows Explorer** ثم اختر الملف أو المجلد الذي تريد مشاركته.
٢. قم بسحب الملف/الملفات إلي المجلد **C:\Users\Public** أو أي مجلد فرعي تحت المجلد **C:\Users\Public** إذا كنت تريد نقل الملفات إلي المجلد **Public**.

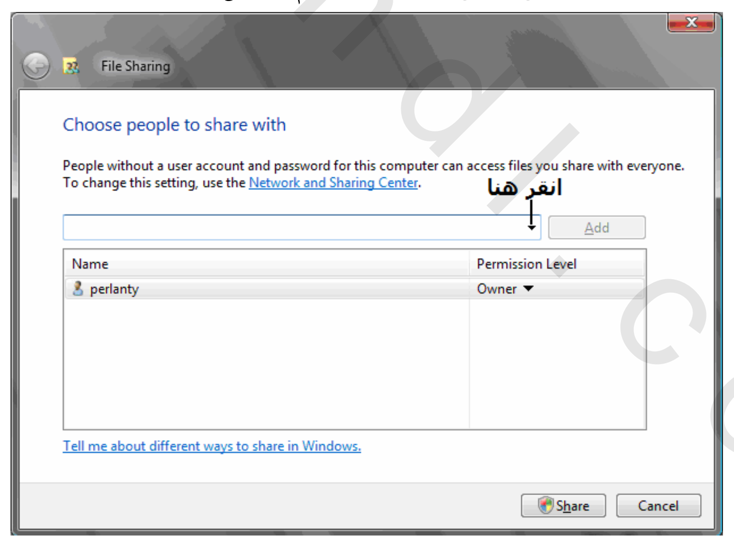
٣. أما إذا كنت تريد نسخ الملفات إلي المجلد **Public** مع الاحتفاظ بها في المجلد الاصلي لديك اضغط مفتاح **Shift** أثناء عملية السحب والإلقاء داخل المجلد **Public**، لا تطلق زر الماوس إلا عندما تري علامة (+) بجوار مؤشر الفأرة.

مشاركة المجلدات بالطريقة التقليدية

لمشاركة المجلدات مع المستخدمين الآخرين بالطريقة التقليدية بدون وضعها في مجلد **Public** "عمومي" سواء كنت تعمل في مجموعة عمل أو نطاق تابع الخطوات التالية:

١. افتح نافذة مستكشف ويندوز **Windows Explorer** ثم حدد المجلد أو المشغل الذي تريد مشاركته سواء كان مشغل الأقراص المرنة **Floppy Drive** أو مشغل الأقراص المدمجة **CD-Drive** الذي تريد مشاركته.

٢. انقر المجلد أو المشغل بزر الماوس الأيمن، ثم اختر الأمر **Share** "مشاركة" سيبدأ معالج مشاركة الملفات **File Sharing** في العمل وتظهر أول خطوة من خطواته وهي الخاصة باختيار الأشخاص الذين ستتشارك معهم. شكل ١٦-٩.



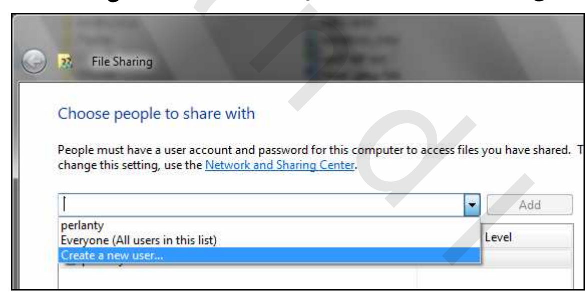
شكل ١٦-٩ أول خطوة من معالج مشاركة البيانات

٣. يجب عليك الآن تحديد من سيشارك في هذا المجلد وما هي صلاحيات المشاركين ، إذا كان خيار حماية المشاركة بكلمة مرور **Password Protecting Sharing**

(الموجود في نافذة **Network and Sharing Center** "مركز الشبكة والمشاركة" السابق شرحها) نشطاً ، فيجب عليك إضافة أسماء كلمات مرور المستخدمين لهذا المجلد.

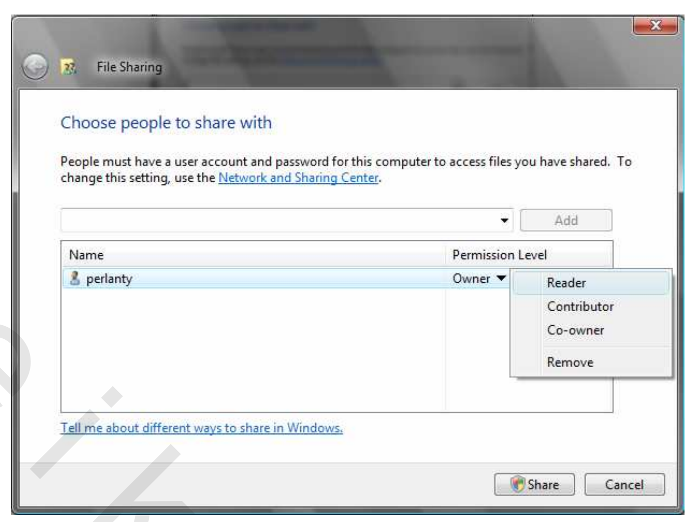
أما إذا كنت لا ترغب في تخصيص أسماء وكلمات مرور للمستخدمين وتريد أن يشارك أي مستخدم للشبكة في هذا المجلد انقر السهم الموجود في طرف المربع الفارغ ثم اختر **Everyone** "كافة المستخدمين في هذه القائمة" من المربع الموجود أعلي المربع الحواري **File Sharing** "مشاركة الملفات" ، ثم انقر زر **Add** "إضافة" سيظهر أسماء المستخدمين الذين اخترقم أو سيظهر الاختيار **Everyone** "كافة المستخدمين في هذه القائمة" .

كما يمكنك إضافة مستخدمين جدد عن طريق اختيار **Create new user** "إنشاء مستخدم جديد" من القائمة الخاصة باختيار المستخدمين. شكل ١٦-١٠



شكل ١٦-١٠ تحديد الأشخاص المشاركين في التعامل مع مجلد المشاركة

٤. بعد تحديد الأسماء يجب عليك اختيار الصلاحيات المخصصة لهؤلاء المستخدمين أو كل منهم علي حده. انقر السهم **Permission Level** "مستوي الأذونات" ثم انقر نوع الوصول الذي تريد السماح به علي النحو التالي: شكل ١٦-١١

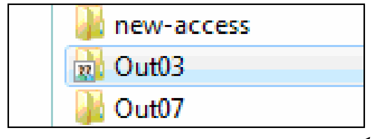


شكل ١٦-١١ اختيار الصلاحيات الخاصة بالمستخدمين

- **Reader** "قارئ" : يكون مسموح لهذا المستخدم بالقراءة والاطلاع فقط.
- **Contributor** "مساهم" : يسمح للمستخدم بالاطلاع وكذلك التعديل أو حتي الحذف .
- **Co-Owner** "شريك المالك" : يسمح للمستخدم بالاطلاع والتعديل حتي في الملفات المضافة من أي مستخدم آخر.

٥. بعد الانتهاء من اختيار المستخدمين وتحديد صلاحياقم انقر الزر **Share** "مشاركة". وعندما يظهر مربع **User Account Control** "التحكم في حساب المستخدم" إذا كنت مسجلاً دخولك كمسئول انقر زر **Continue** "متابعة"، وإلا اكتب كلمة مرور المسئول ثم انقر **OK** "موافق".

٦. بعد أن تتم مشاركة المجلد، انقر الزر **Done** "تم". يتغير رمز المجلد في قائمة المجلدات ولوح المحتويات يتغير رمز المجلد إلي رأس وأكتاف لشخصين. كما في شكل ١٦-١٢



شكل ١٦-١٢ ظهور رمز المشاركة بجوار المجلد

مشاركة مشغلات الأقراص

كما تحدثنا سابقاً أن المشاركة تتم للمجلدات الجذرية **Root Folders** وليس المجلدات الفرعية **Subfolders** وبالتالي تستطيع جعل أجزاء أو مشغلات الأقراص في جهازك مشغلات مشتركة وقد يفيدك هذا خصوصاً في حالات تحويل مشغلات الأقراص المرنة **Floppy Disk** ومشغلات الأقراص المدمجة **CD-Rom** أو مشغلات الأقراص الفلاشية **USB disk drives** إلي مشغلات مشتركة .

فإذا قمت بمشاركة مشغل الأقراص المدمجة **CD-Rom** تستطيع تشغيل الاسطوانة التي بداخل المشغل من علي أي جهاز داخل الشبكة ، فإذا كنت تريد مثلاً تثبيت برنامج علي جهاز من أجهزة الشبكة وكان مشغل الأقراص الخاص بهذا الجهاز غير صالح للعمل تستطيع عن طريق مشاركة المشغل في الشبكة تثبيت هذا البرنامج من خلال أي جهاز آخر في الشبكة مثبت عليه مشغل أقراص جيد تقوم بمشاركته لكل أجهزة الشبكة.

يجب عليك أن تعرف أن **Windows** عندما تشارك أي جزء من أجزاء قرصك الصلب يصبح أسمه عند المشاركة **C$** أو **D$** وهكذا. لن تظهر أمامك هذه العلامة عند استعراض أجزاء الأقراص ولكنها توضع مخفية فقط. لكي توضح لـ **Windows** أن هذه الأجزاء هي أجزاء مشاركة في الشبكة أما ملفات المشاركة فيتم حفظ اسمها بنفس مفهوم التسمية الذي شرحناه سابقاً فيصبح المجلد عند مشاركته بالاسم **\\ Berl\C$** وهكذا.

مشاركة الطابعات

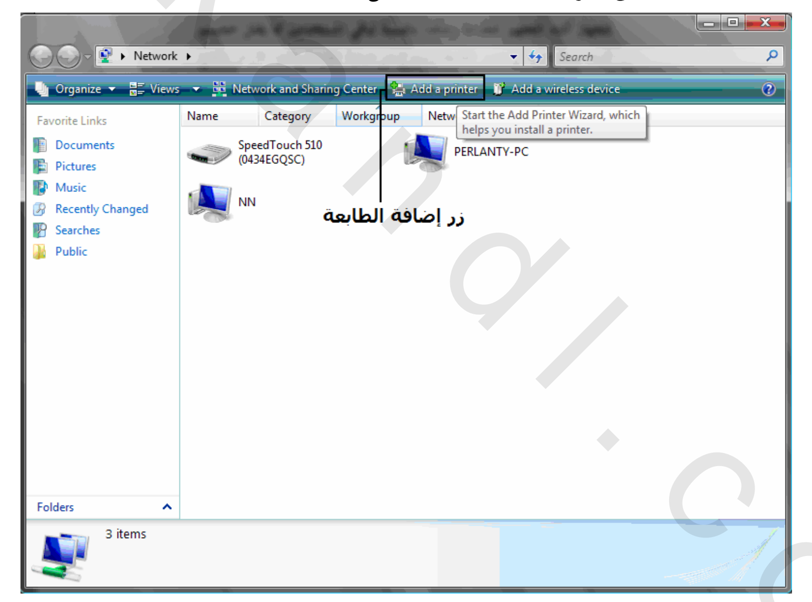
لعل من أهم استخدامات الشبكة هو توفير الموارد والأجهزة وخصوصاً الطابعات فإذا كنت مستخدماً في شبكة لشركة كبيرة أو كنت مستخدماً في مجموعة عمل صغيرة أو حتي في منزلك عندما يكون لديك جهازي كمبيوتر متصلين ببعضهما فإن استخدام نفس الطابعة يوفر عليك شراء طابعة خاصة لكل منهما.

إعداد طابعات الشبكة

لكي تستخدم طابعة مشتركة يجب عليك إضافة اختصار الطابعة إلي نافذة مدير الطابعات في جهازك ، الطريقة المثلي لعمل ذلك هي البحث عن الطابعات المشتركة الموجـــودة في شبكتك ، عندما تجد الطابعة المشتركة التي تريدها قم بنقرها بزر الماوس الأيمن ثم اختــر الأمر **Open** لتستطيع التعامل معها من خلال جهازك.

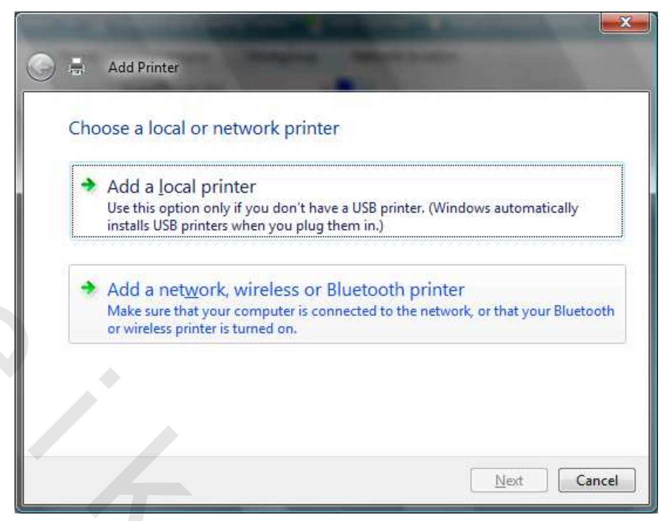
كما يمكنك استخدام معالج إضافة الطابعات لعمل ذلك، لمتابعة معالج إضافة الطابعـــات تابع الخطوات التالية :

١. من نافذة مستكشف الشبكة **Network Explorer** ، انقر الـــزر **Add Printer** "إضافة الطابعة" من شريط الأدوات . شكل ١٦-١٣



شكل ١٦-١٣ زر **Add a Printer** "إضافة الطابعة" في نافذة الشبكة **Network Explorer**

٢. سيظهر المربع الحواري **Add Printer** "لإضافة طابعة" لتختار منه إذا كانت طابعة محلية أم طابعة شـــبكة ، انقـــر الارتبـــاط **Add a Network, Wireless, or Bluetooth Printer** "إضافة طابعة شـــبكة، أو طابعـــة لاســـلكية، أو طابعـــة Bluetooth" . شكل ١٦-١٤

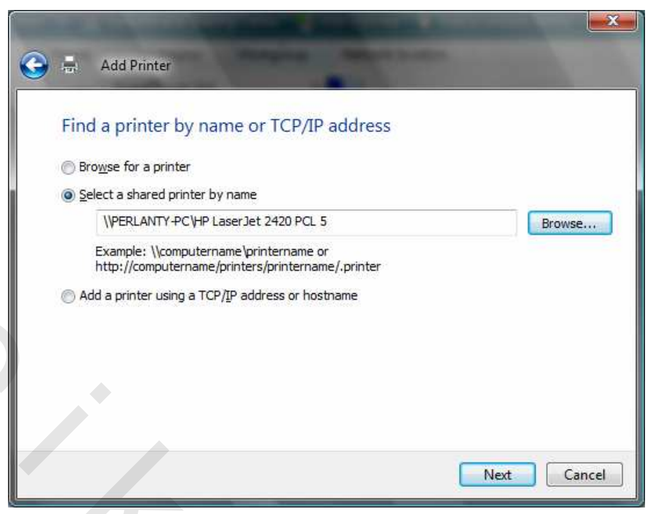


شكل ١٦-١٤ اختيار تثبيت طابعة شبكة

٣. سيقوم **Windows** بالبحث عن الطابعات المثبتة لديك أو في الشبكة ، إذا لم تجد الطابعة التي تريدها في قائمة الطابعات الظاهرة ، انقر الارتباط **The Printer That I Want Isn't Listed** "الطابعة التي ابحث عنها ليست مدرجة".

٤. سيظهر مربع حواري آخر لتكتب فيه اسم ومكان الطابعة التي تريد مشاركتها. إذا لم تكن تعرف اسم الطابعة التي تريدها انقر زر **Browse** "استعراض" ستظهر نافذة تعرض كل أجهزة الكمبيوتر المتصلة معك وكل الطابعات المثبته مع هذه الأجهزة

٥. بعد الانتهاء من تحديد مكان واسم الطابعة انقر زر **Next** "التالي" للعودة إلي المربع الحواري وستجد فيه اسم ومكان الطابعة المحددة . شكل ١٦-١٥



شكل ١٦–١٥ تحديد مكان واسم الطابعة المراد مشاركتها

٦. عندما تنتهي من تعريف طابعة المشاركة، انقر **Next** "التالي" لإنهاء الإعداد، وسيقوم **Windows** بإعداد الطابعة مثلما يفعل مع الطابعة المحلية تماماً.

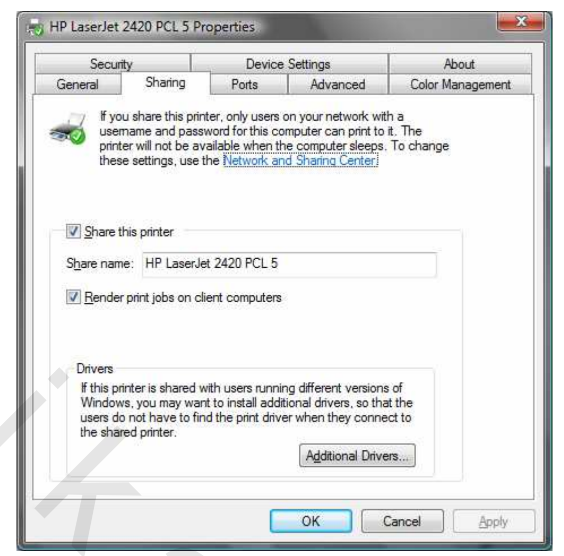
مشاركة الطابعات

كما قلنا يمكنك مشاركة الطابعة المحلية الموجودة علي جهازك ليتمكن أي مستخدم للشبكة من الطباعة عليها، لتمكين مشاركة الطابعة تابع الخطوات التالية:

١. افتح قائمة **Start** "ابدأ" ثم اختر **Network** "الشبكة" ، ثم اختر **Network and Sharing Center** "مركز الشبكة والمشاركة"، ستظهر النافذة **Network and Sharing Center** "مركز الشبكة والمشاركة".

٢. من الجزء **Sharing and Discovery** "المشاركة والاكتشاف" الموجود في وسط النافذة انقر السهم المجاور للعنوان **Printer Sharing** "مشاركة الطابعة" ، ثم قم بتنشيط الخيار **Turn On Printer Sharing** "إيقاف تشغيل مشاركة الطابعات" ثم انقر **Apply** "تطبيق" .

٣. سيظهر المربع الحواري الخاص بمشاركة الطابعة ويظهر فيه التبويب **Sharing** "مشاركة" هو التبويب النشط. شكل ١٦–١٦



شكل ١٦-١٦ التبويب Sharing "مشاركة" في مربع خصائص الطابعة

٤. انقر الاختيار Share this Printer "مشاركة هذه الطابعة" ثم ادخل اسم الطابعة علي الشبكة ثم انقر OK "موافق" للانتهاء من مشاركة الطابعة، سيتم مشاركة الطابعة وخصوصاً إذا كانت كل الأجهزة التي تعمل علي الشبكة تعمل بنظام Windows Vista أو XP أو 2000.

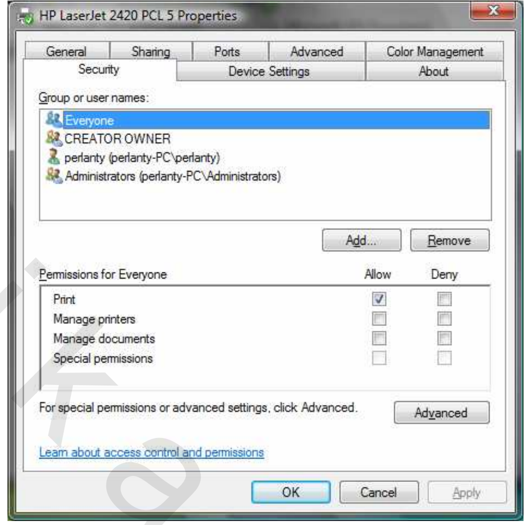
تحديد صلاحيات الطباعة

بعد مشاركة الطابعة علي الشبكة قد تحتاج لإعطاء كل مستخدم صلاحيات معينة لعملية الطباعة لعمل ذلك تابع الخطوات التالية :

١. تأكد أن مربع خصائص الطابعة ما زال مفتوحاً أمامك (راجع شكل ١٦-١٦)، قم بتنشيط التبويب Security "الأمان"، سيظهر التبويب Security "الأمان" نشطاً وستلاحظ وجود الصلاحيات المسموح بها للمستخدمين أسفل التبويب وهي:

- Print "طباعة" : للسماح للمستخدم بالطباعة.
- Mange Printers "إدارة الطابعات" : للسماح بالتغيير في إعدادات الطابعة ومشاركتها أو عدم مشاركتها في الشبكة.

- **Manage Documents "إدارة المستندات" : لإلغاء أو تأجيل مهام الطباعة من المستخدمين الآخرين. شكل ١٦-١٧**



شكل ١٦-١٧ تحديد مهام المستخدمين للطابعة علي الشبكة

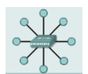
٢. **بعد الانتهاء من الإعدادات المناسبة انقر OK "موافق" .**

ملخص الفصل

تعرفنا في هذا الفصل علي كيفية مشاركة موارد الشبكة باعتبارها هدفاً ضرورياً يسعي إليه مستخدمو الشبكات. وشرحنا كيف يتم تنظيم صلاحيات مشاركة الشبكة والتعامل معها من قبل جميع المستخدمين. أوضحنا في خطوات عملية كيف يتم مشاركة موارد الشبكة المختلفة وتشمل المجلدات والملفات، ومشغلات الأقراص، والطابعات.

تدريبات

١. **اتبع خطوات مشاركة الملفات بمجلد عمومي وخطوات مشاركة الطابعات لكي تستخدم طابعة مشتركة متصلة بمجموعة كمبيوترات ثم أطلع مدربك علي نتيجة عملك.**



الباب السادس
التوجيه والشبكات الفرعية

الفصل السابع عشر : عنونة IP

الفصل الثامن عشر : التوجيه والموجهات

الفصل التاسع عشر : الشبكات الفرعية



الفصل السابع عشر

عنونة IP

*تناولنا في الفصل السابع بروتوكول **TCP/IP** وشرحنا الطبقات التي يتكون منها ووظيفة كل طبقة، وأنهينا الفصل بمقارنة بين نموذج **TCP/IP** ونموذج **OSI**. ولكن هذا ليس كل شيء سنتعرف في هذا الفصل على أمور غاية في الأهمية تشمل :*

- *فهم عنونة **IP** (**IP Addressing**)*
- *فهم أقنعة الشبكة*
- *عنونة **IPV4***
- *الحصول علي عناوين **IP***
- *عناوين **IP** المحجوزة*
- *عناوين **IP** العامة والخاصة*
- *عنونة **IPV6** ومقارنتها مع **IPV4***
- *عناوين **IP** الثابتة والمتغيرة*
- *عناوين **IP** الثابتة*
- *عناوين **IP** المتغيرة وبروتوكول **DHCP***

TCP/IP اختصار للعبارة **Transmission Control Protocol/ Internet Protocol** ويمكن ترجمتها "بروتوكول التحكم في الإرسال / بروتوكول الانترنت" وهو عبارة عن مجموعة من البروتوكولات المستخدمة في ربط الشبكات والتي انبثقت عن الانترنت. وخضعت لتعديلات كثيرة علي مدي العقدين الماضيين، حتي أصبحت في النهاية أداة ممتازة لنقل كمية كبيرة من المعلومات بصورة يمكن الاعتماد عليها وبسرعة عبر شبكة اتصال معقدة. لقد تم مزج كلاً من **TCP** و **IP** في البداية، وتم فصلهما فيما بعد لتحسين كفاءة النظام. سبق أن ألقينا نظرة مختصرة علي مجموعة من بروتوكولات **TCP/IP** وكيفية ارتباطها بنموذج **OSI** (راجع الفصل السابع من هذا الكتاب).

فهم عنونة IP (IP Addressing)

لكي يتم الاتصال بين أي جهازين، يجب أن يكون كلاهما قادراً على التعرف على الآخر. وعادة يتم تخصيص عنوان لكل جهاز موجود على الشبكة. ويسمح هذا النظام لأجهزة الكمبيوتر الأخرى الموجودة علي الشبكة بالتعرف على هذا الجهاز. بعبارة أخري يجب تخصيص عنوان مميز لكل جهاز كمبيوتر موجود علي شبكة تستخدم **TCP/IP** . يسمي هذا العنوان **IP Address** أو "عنوان **IP**" . من الضروري لأي جهاز موصل بالشبكة أن يكون له عنوان **IP** سواء كانت شبكة محلية أو موسعة كالإنترنت مثلاً. عندما درسنا نموذج **OSI** رأينا أن طبقة الشبكة (**Network Layer**) مسئولة عن الاتصال بين جهازين مهما كان موقعهما، وبما أن بروتوكول **IP** هو العمود الفقري لطبقة الشبكة. فالاستغناء عن هذا البروتوكول يؤدي إلي عزل الجهاز عن الشبكة . بعبارة أخري يتيح "عنوان **IP**" لكل جهاز موجود علي الشبكة أن يتعرف علي باقي الأجهزة.

أيضاً يتم تعيين عنوان مادي مميز لجميع أجهزة الشبكة يسمي هذا العنوان **MAC Address** "عنوان **MAC**" وتقوم الشركات المصنعة لبطاقات الشبكة **(NIC)** بتعيين هذا العنوان. الجدير بالذكر أن عناوين **MAC** تعمل عند الطبقة الثانية من نموذج **OSI**.

ولكن ما هو شكل عنوان **IP**. هل هو مثل العنوان البريدي (رقم صندوق بريد وكود للبلد مثلاً) أو هو مثل عنوان البريد الالكتروني (**e-mail**) يبدأ باسم الشخص متبوعاً بعلامة **@**

ثم اسم الشركة. في الحقيقة لا هذا ولا ذاك ....

عنوان IP (IP Address) عبارة عن سلسلة من الآحاد والاصفار عددها ٣٢ يقال عنها bits يتم تقسيم الـ 32 bits إلي أربعة أجزاء بواسطة نقاط يحتوي كل جزء علي 8 Bits. (راجع الفصل الثالث من هذا الكتاب) يمكن أن يأخذ عنوان IP هذا الشكل علي سبيل المثال :

11111111 00001111 0100010 01000000

وهو يشتمل علي عينة لرقم يتكون من 32 bits. يطلق علي هذه الصيغة Dotted Binary Notation "التمثيل الثنائي ذو النقاط"

ولتسهيل التعامل مع عنوان IP، فإنه يكتب عادة علي شكل أربعة أرقام عشرية مفصولة بعلامة النقطة (.) مثلاً يمكن أن يخصص هذا العنوان لأحد أجهزة الكمبيوتر وهو بالفعل

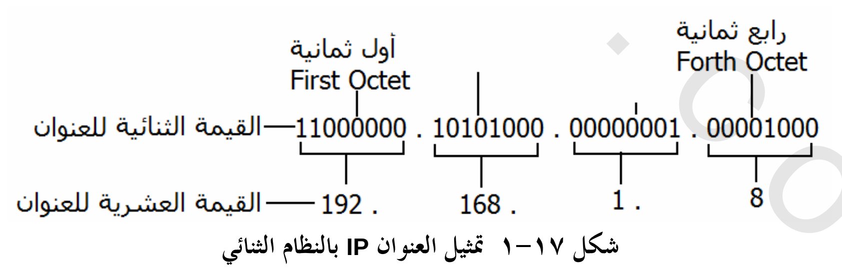
IP Address : 192.168.1.2

بينما يمكن تخصيص هذا العنوان لجهاز آخر : **128.10.2.1**

ويسمي كل جزء من العنوان Octet ومعناه ثمانية بتات . أي أنه يتكون من ثمانية أرقام ثنائية، فمثلاً هذا العنوان 192.168.1.8 يمكن تمثيله بالنظام الثنائي هكذا.

11 000000 . 10101000 . 00000001. 00001000

وبالطبع هذه الطريقة وهي التمثيل العشري أسهل بكثير من طريقة النظام الثنائي الذي يحتوي على آحاد وأصفار. (انظر شكل ١٧-١)



شكل ١٧-١ تمثيل العنوان IP بالنظام الثنائي

تسمي هذه الطريقة Dotted Decimal Notation "التمثيل العشري ذو النقاط". كلا الرقمين العشري والثنائي في المثال السابق يحملان نفس القيمة، إلا أن التمثيل العشري أسهل في فهمه وفي المقابل فإن سلسلة الآحاد والأصفار الطويلة تسبب في الغالب أخطاء.

انظر شكل ١٧–٢ . طبعا من السهل أن تتعرف على العلاقة بين الرقم **192.168.1.8** والرقم **192.168.1.9** من أن تتعرف علي القيمة المقابلة بالنظام الثنائي وهي كما يلي

11 000000 . 10101000 . 00000001 . 00001000

و **11 000000 . 10101000 . 00000001 . 00001001**

راجع كيفية التحويل من النظام الثنائي إلي النظام العشري أو التحويل من النظام العشري إلي النظام الثنائي في الفصل الثالث)

Binary : 11000000.10101000.00000001.00001000 and 11000000.10101000.00000001.00001001
Decimal : 192.168.1.8 and 192.168.1.9

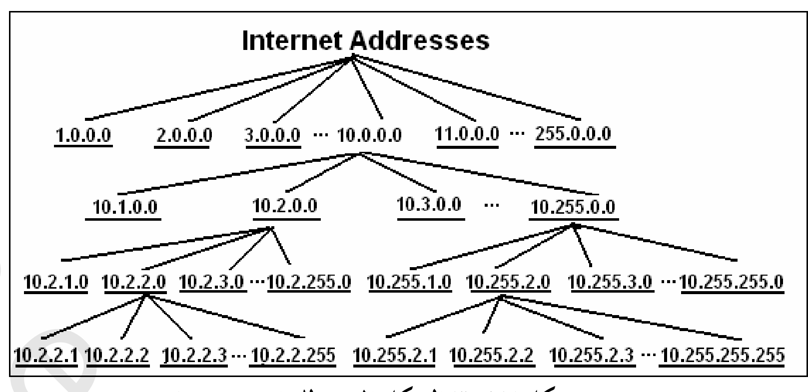
شكل ١٧–٢ العنوان بالنظام الثنائي والنظام العشري

عنونة IPV4

يستخدم الموجه عنوان **IP** لتمرير حزم البيانات من شبكة المصدر (المرسل) إلي شبكة الهدف (المستقبل) . ويجب أن تشتمل الحزمة على معرف أو عنوان لكل من شبكة المصدر (المرسل) والوجهة (المستقبل) . يستخدم الموجه عناوين **IP** لشبكة الوجهة لتسليم حزمة البيانات إلي الشبكة المطلوبة.

وعندما تصل الحزمة إلي موجه متصل بشبكة الوجهة، فإن الموجه يستخدم عنوان **IP** للتعرف علي الجهاز المحدد علي الشبكة. وهو يشبه النظام المستخدم في إيصال رسائل البريد منذ زمن طويل. حيث يستخدم رقم صندوق البريد لتوجيه الرسالة إلي مكتب البريد في مدينة الوجهة. ويتعرف مكتب بريد الوجهة علي اسم الشارع للتعرف على عنوان المرسل إليه داخل المدينة.

وكما يتضح من شكل ١٧–٣ أن كل مجموعة من ثمانية بتات يخصص لها مديً من **0** إلي **255**، وكل واحدة من الثمانية تنقسم إلي ٢٥٦ مجموعة فرعية، ثم تنقسم كل مجموعة إلي ٢٥٦ مجموعة فرعية آخري، حيث تحمل كل مجموعة ٢٥٦ عنواناً. بالإشارة إلي عنوان المجموعة والذي يوجد مباشرة فوق المجموعة كما في الشكل ، يمكن اعتبار كل المجموعات المتفرعة من العنوان على شكل هرمي وحدة واحدة .



شكل ١٧-٣ الشكل الهرمي للعناوين

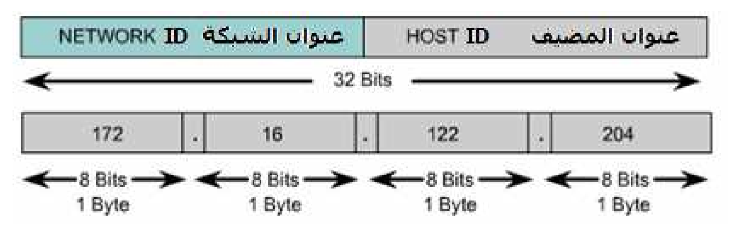
يجب أن يكون كل رقم من الأرقام التي يتكون منها كل عنوان من العناوين الموجودة في الشكل مميز أو فريداً داخل البناء الهرمي، لأن تكرار العناوين يجعل عملية توجيه العناوين أمراً مستحيلاً. وكما ستعرف بعد قليل أن الجزء الأول يعِّرف عنوان شبكة النظام "**Network**" أما الجزء الثاني ويسمي **Host Part** "جزء المضيف" فإنه يعِّرف الجهاز نفسه الموجود داخل الشبكة.

فئات عناوين IP

لقد تم تقسيم **IP** إلي مجموعات أو فئات تسمى **Classes** ولكل فئة قناع شبكة فرعية افتراضي، وكما أوضحنا من قبل تتكون عناوين **IPV4** من **32** بت من المعلومات ، وتتم كتابتها برموز عشرية نقطية مكونة من أربع ثمانيات بالتنسيق **X.X.X.X**. وينقسم كل عنوان **IP** يتكون من **32 bit** إلي جزئيين.

- الجزء الأول لتعريف الشبكة بموقع الجهاز علي الشبكة ويسمي **Network ID** وأحياناً **Network Address** ومعناها معِّرف الشبكة أو عنوان الشبكة.
- الجزء الثاني يعرف الجهاز نفسه ويسمي **Host ID** وأحياناً **Host Address** ومعناها معِّرف المضيف أو عنوان المضيف.

ويأخذ كل جزء ثمانية (**Octet**) أو ثمانيات متجاورة انظر شكل ١٧-٤.

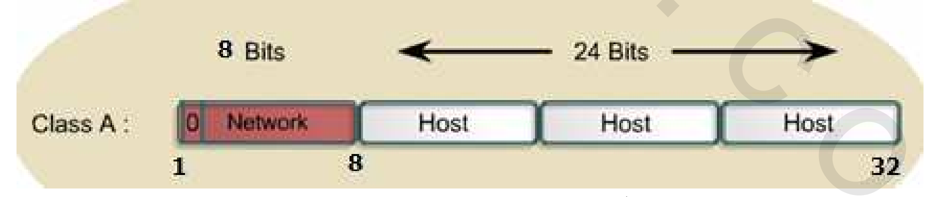


شكل ١٧-٤ تقسيم عنوان الشبكة إلي جزء الشبكة والجزء المضيف

وتنقسم عناوين **IP** إلي خمسة فئات منها ثلاث فئات قابلة للاستخدام (قابلة للاستخدام من أجل التعيين لأجهزة الشبكة) وهى **A** و **B** و **C** وهذه سيتم التركيز عليها بينما سنشير باختصار إلي فئتي **D** و **E** .

نوضح فيما يلي فئات عناوين **IP** والمدي المخصص لكل منها.

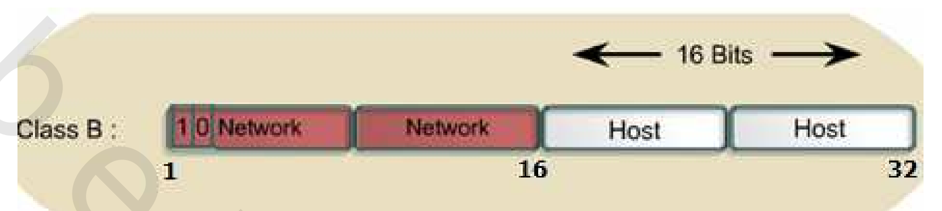
الفئة أ (Class A) : تستخدم مع الشبكات الضخمة. حيث توفر أكثر من ١٦ مليون عنوان مضيف (١٦٧٧٧٢١٤ عنوان) لكل شبكة اتصال، ولذلك فهي تستخدم مع الشبكات الكبيرة جداً يظهر في شكل ١٧-٥ تنسيق العنوان من فئة **A**. يستخدم **Class A** أول ثمانية بتات من عناوين **IP** للإشارة إلي عنوان الشبكة (**Network ID**). والثمانيات الثلاث الباقية (أي الـــ ٢٤ بت المتبقية) للإشارة إلي عنوان المضيف (**Host ID**) . وتأخذ أول **bit** في أول ثمانية (**Octet**) في **Class A** القيمة **0** ومجالها يكون من **00000001** إلي **011111111** وتعني بالنظام العشري من ١ إلي ١٢٧ . وعلي ذلك فإن أعلي رقم يمكن تمثيله هو **01111111** وتساوي بالنظام العشري **127**.



شكل ١٧-٥ تنسيق عنوان **IP** من الفئة **A**

لاحظ أن الرقم صفر والرقم ١٢٧ محجوزان ولا يستخدمان كعناوين للشبكة. والعناوين التي تحتوي عليها أول ثمانية من **Class A** يقع بين ١ و ١٢٦. يعني يمكن أن يكون هناك ١٢٦ شبكة من الفئة **A** .

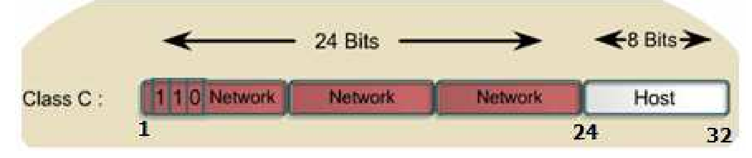
الفئة ب (Class B) : وهى تناسب المؤسسات المتوسطة إلي الكبيرة شكل (١٧-٦). يستخدم Class B أول ثمانيتين من الثمانيات الأربع للإشارة إلي عنوان الشبكة. بينما تشير الثمانيتان الأخريان إلي عناوين المضيف.



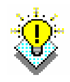
شكل ١٧-٦ تنسيق عنوان IP من الفئة B

عادة تحتوي أول ٢بت (2 bit) من أول ثمانية من عناوين Class B علي 10، وتحتوي البتات الستة الباقية من أول ثمانية علي آحاد أو أصفار. وعلى ذلك فإن أقل رقم يمكن وضعه داخل Class B هو 10000000 وتساوي بالنظام العشري 128 .أما أكبر رقم يمكن وضعه فهو 10111111 وتساوي بالنظام العشري 191. نفهم من ذلك أن أي عنوان يقع بين ١٢٨و١٩١ في أول ثمانية هو عنوان يخص الفئة B (Class B). توفر ما يصل إلي ٦٥٥٣٤ عنوان مضيف لكل شبكة ، ويوجد ١٦٣٨٢ عنوان شبكة اتصال من الفئة B.

الفئة ج (Class C) : صممت هذه الفئة لخدمة المؤسسات الصغيرة التي لا يزيد عدد المضيفين بها عن 254 مضيفاً في كل شبكة اتصال شكل (١٧-٧). تبدأ بالرقم الثنائي 110 ولهذا فإن أقل رقم يمكن وضعه فيها هو 11000000 وتساوي بالنظام العشري ١٩٢، أما أكبر رقم يمكن أن يوضع بها فهو 11011111 وتساوي بالنظام العشري 223. وعلى ذلك نفهم أن أي رقم يقع بين ١٩٢ و ٢٢٣ في أول ثمانية ، معناه أنه ينتمي إلي الفئة C (Class C). يوجد أكثر من ٢ مليون (٢٠٩٧١٥٠) عنوان شبكة من الفئة C.

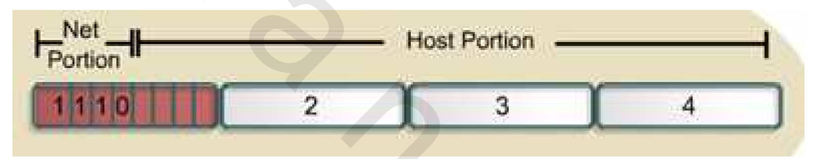


شكل ١٧-٧ تنسيق عنوان IP من الفئة C



الجدير بالذكر أن عناوين IP من Class A لم تعد متوفرة ، أما الفئة B فيتم تعيينها للشركات الكبري. تعد شركة Microsoft من Class B. فإذا لم تكن تعمل في مؤسسة كبيرة، فلن تري إلا عناوين Class C

الفئة د (Class D) : صممت هذه الفئة لتتيح تعدد القوالب (Mullicasting) في عناوين IP شكل (١٧-٨) وهو عنوان شبكة فريد يوجه الرزم إلي مجموعة محددة سلفاً من عناوين IP. ولهذا فإن محطة واحدة يمكنها نقل مجموعة من البيانات إلي عدة مستلمين.تبدأ أول أربعة بت (4 bits) من الفئة D بالرقم الثنائي 1110، ولهذا فإن مدى أول ثمانية عناوين من الفئة D يقع بين 11100000 و 11101111 أو بالنظام العشري ٢٤٤ و ٢٣٩. وعلي ذلك فإن أي عنوان IP يبدأ بمدي يقع بين ٢٢٤ و ٢٣٩ في أول ثمانية يعتبر ضمن Class D.



شكل ١٧-٨ تنسيق عناوين IP للفئة D

الفئة هـ (Class E) : هذه الفئة محجوزة لمؤسسة IETF ومعناها Internet Engineering Task Force "قوة مهام هندسة الانترنت" شكل (١٧-٩) لتجري عليها أبحاثها.



شكل ١٧-٩ تنسيق عنوان IP للفئة E

ولذلك فليس لها عناوين مستخدمة في الانترنت. يخصص لأول أربعة بت (4bits) من أول ثمانية دائما القيمة 1111 ولذلك فإن مدي أول ثمانية من هذه الفئة يقع بين 11110000 و 11111111 وتساوي بالنظام العشري ٢٤٠ و ٢٥٥.

يوضح شكل ١٧-١٠ مدي عناوين IP في أول ثمانية بكل من النظام الثنائي والعشري

لكل فئة من فئات عناوين IP .

IP address class فئة عنوان IP	IP address range مدي عناوين IP عشري ثنائي
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)

شكل ١٧–١٠ يتم تحديد الفئة بناء علي القيمة العشرية لأول ثمانية، تذكر أن العنوان 127 محجوز ولا يمكن تخصيصه لأي شبكة.

فهم أقنعة الشبكة الفرعية

توفر أقنعة الشبكة الفرعية الافتراضية بعض الإرشادات المرئية الواضحة وقد سبق أن قلنا أن لكل فئة قناع شبكة افتراضي علي النحو التالي:

الفئة A (Class A) : 255 . 0 . 0 . 0

الفئة B (Class B) : 255 . 255 . 0 . 0

الفئة C (Class C) : 255 . 255 . 255 . 0

انظر إلي قناع الشبكة الفرعية A . ماذا تلاحظ؟

ستلاحظ أن 255 يظهر فقط في النطاق الثمانى الأول. يعني أن البتات الثمانية المقابلة للرقم العشري 255 سوف تكون هكذا: 11111111 أي أن البتات الثمانية في حالة ON (تم تشغيلها) . يخبر ذلك جهاز الكمبيوتر بأن النطاق الثماني الأول يحتفظ بمعلومات الشبكة، تخفى البتات الثمانية التي تم تشغيلها في قناع الشبكة الفرعية النطاق الثماني الأول من أي عنوان IP في الفئة A . لاحظ أن النطاقات الثمانية المتبقية في قناع الشبكة الفرعية للفئة A هي أصفار. ويعني أن النطاق الثانى والثالث والرابع لا توجد بها معلومات .

معني هذا أن في الشبكة من الفئة A تستخدم ٨ بتات لتحديد معلومات الشبكة وتستخدم البتات الـــ٢٤ الباقية لعناوين المضيف أو الأجهزة. هذه الـــ ٢٤ بت تعطينا احتمالات

للعناوين الفرعية تصل حتي أكثر من ١٦ مليون احتمال .

في شبكات الفئة B (Class B) يتم استخدام كل من النطاق الثماني الثالث والرابع لعناوين المضيف أو الأجهزة ، لأن النطاقان الأول والثاني يتم اخفاؤهما بواسطة قناع الشبكة الفرعية وحيث يبلغ طول النطاق الثالث والرابع ١٦بت وهي البتات المتوفرة لعناوين الوحدات الفرعية، فإن شبكات الفئة B ستوفر عناوين وحدات فرعية تصل إلي نحو ٦٥٠٠٠ عنوان. أما في شبكات الفئة C . فكما تلاحظ أن النطاق الثماني الرابع فقط هو الذي يتم حجزه لعناوين الوحدات الفرعية، بينما تستخدم النطاقات الثمانية الثلاثة الأخرى لمعلومات الشبكة. ولهذا السبب توفر شبكات الفئة C عناوين IP عددها ٢٥٤ فقط وهو عدد عناوين أقل بكثير من عناوين الشبكات السابقة.

والخلاصة أنه في حين تخصص الفئة A (Class A) للشبكات الكبيرة، تخصص الفئة B (Class B) للشبكات المتوسطة، وتخصص الفئة C (Class C) للشبكات الصغيرة.

يوضح شكل ١٧-١١ عدد الشبكات المخصصة لكل فئة من فئات عناوين IP وعدد الأجهزة التي يمكن توصيلها بكل شبكة.

Address Class فئات العنوان	Number of Network عدد الشبكات	Number of Host Per Network عدد الأجهزة في كل شبكة
A	254*	16.777.216
B	16.384	65.535
C	2.096.152	254

شكل ١٧-١١ عدد الشبكات المخصصة لكل فئة من فئات عناوين IP
وعدد الأجهزة التي يمكن توصيلها بكل شبكة

من هذا نفهم أنه يجب توصيف كل جهاز علي الشبكة باستخدام عنوان IP فريد وقناع الشبكة الفرعية المناسب. مع ملاحظة أنه لا يمكن أن تكون قيم كل البتات في عنوان الشبكة أو المضيف أصفاراً ، كما لا يمكن أن تكون قيم كل البتات في عنوان الشبكة أو المضيف آحاداً.

هل تعرف من أين نحصل علي عناوين IP ؟

الحصول علي عناوين IP

توجد مؤسسات حول العالم تتولي إدارة عنونة IP. أكبر مؤسسة مسئولة عن تأجير عناوين IP هي The American Registry For Internet Numbers وتختصر هكذا ARIN ومعناها " السجل الأمريكي لأرقام الأنترنت" وهي مؤسسة خيرية تم تأسيسها لتسجيل (وإدارة) عناوين IP لمناطق أمريكا الشمالية والجنوبية ومنطقة الكاريبي وصحراء أفريقيا أما المؤسسة المسئولة عن إدارة عنونة IP في أوربا والشرق الأوسط والمناطق الافريقية التي لا تديرها ARIN فهي مؤسسة RIPE Network Coordination Center "مركز تنسيق شبكات RIPE" أما مناطق الباسيفك الأسيوية فتديرها مؤسسة أخري، تحتفظ ARIN (أو غيرها من المؤسسات التي تدير عنونة IP) بنطاق من العناوين في الفئات الثلاثة A و B وC. وتشمل هذه النطاقات ما يلي :

- الفئة A (CLASSE A): من **10.0.0.0** إلي **10.255.255.255** بقناع شبكة فرعية **255.0.0.0**
- الفئة B (CLASSE B): من **172.16.0.0** إلي **172.31.255.255** بقناع شبكة فرعية **255.255.0.0**
- الفئة C (CLASSE C): من **192.168.0.0** إلي **192.168.255.255** بقناع شبكة فرعية **255.255.255.0**

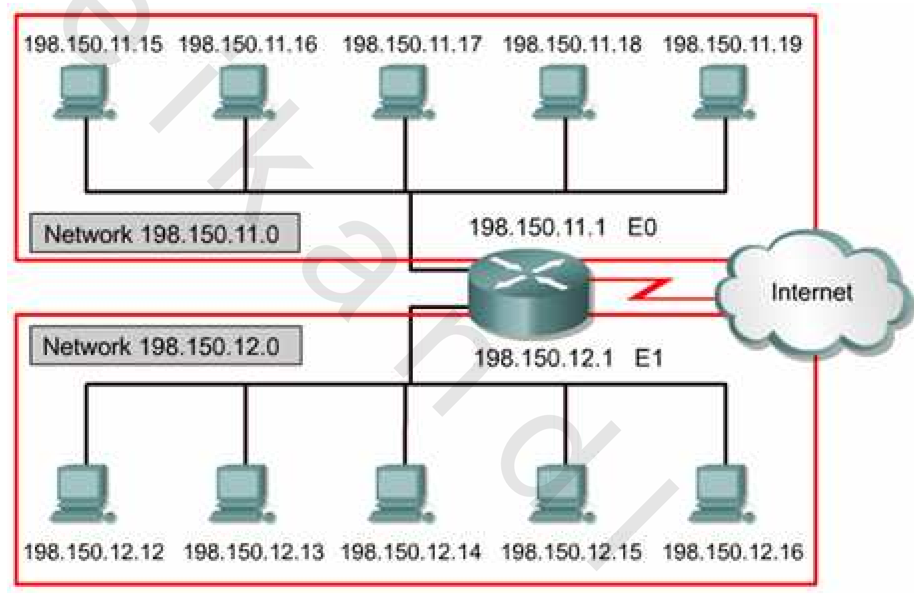
وعادة يتم تأجير عناوين IP ثابتة من مزود خدمة الانترنت مباشرة إلا إذا كنت في مؤسسة كبيرة جداً فيمكنك في هذه الحالة التوجه إلي المؤسسة المسئولة عن تأجير العناوين (مثل ARIN أو غيرها) حيث أن الحد الأدنى من العناوين الذي يمكن تأجيره من مؤسسات تأجير العناوين مباشرة هو 4.096 عنوان.

عناوين IP المحجوزة

توجد بعض عناوين IP لا يمكن تخصيصها لأي وحدة أو جهاز كمبيوتر علي الشبكة. وتشمل عناوين المضيف المحجوزة ما يلي :

- **Network Address** " عنوان الشبكة" لأنه يستخدم لتعريف الشبكة نفسها.

في شكل ١٧-١٢ في القسم الموجود به المستطيل الذي يحتوي علي الشبكة **198.150.11.0** وهو القسم العلوي من الشكل ، فإن البيانات المرسلة إلي أي مضيف أو جهاز علي هذه الشبكة (من **198.150.11.1** إلي **198.150.11.254**) سيتم رؤيتها خارج الشبكة المحلية علي أنها **198.150.11.0** . وسيتم رؤية أرقام المضيف علي الشبكة المحلية فقط.

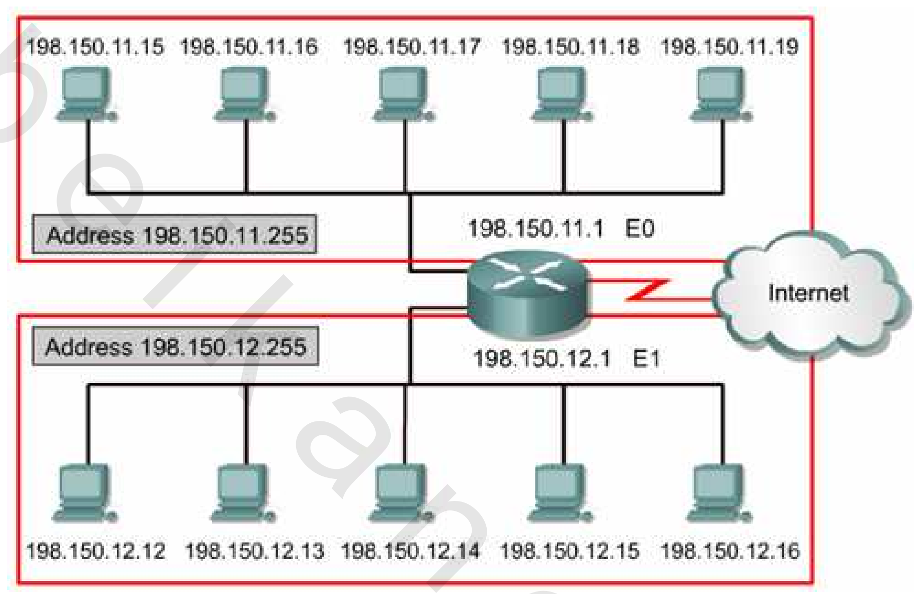


شكل ١٧-١٢ عناوين الشبكة **Network Addresses**

وأيضاً القسم الذي يشتمل علي المستطيل الذي يحتوي على الشبكة **198.150.12.0** (وهو القسم السفلي من الشكل) يعامل نفس المعاملة، فسوف تُري الشبكة من الخارج على أنها **198.150.12.0**.

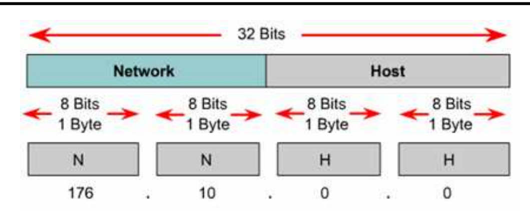
- **Broadcast Address** "عنوان الإرسال (البث)" يستخدم لإرسال حزمة بيانات إلي جميع الوحدات الموجودة على الشبكة. في شكل ١٧-١٣ الجزء الموجود به المستطيل العلوي يمثل عنوان بث **(Broadcast Address)** هو **198.150.11.255**. وسيتم قراءة البيانات المرسلة إلي عنوان بث **(Broadcast**

Address) بواسطة جميع المضيفين الموجودين علي الشبكة (يعنى في المدي من 198.150.11.1 إلي 198.150.11.254). وبالمثل يتم معاملة الشبكة الموجودة في المستطيل السفلي.



شكل ١٧–١٣ عناوين البث Broadcast Address

عنوان IP الذي يحتوي علي أصفار (بالنظام الثنائي) في جميع أماكن البتات المخصصة للمضيف يتم حجزه لعنوان الشبكة (Network Address) . فعلي سبيل المثال في شبكة من نوع Class A يعتبر العنوان 113.0.0.0 هو عنوان IP للشبكة. (ويعرف بمعِّرف الشبكة أو Network ID). ويستخدم الموجه عنوان شبكة IP (Network IP Address) عندما يعيد تحويل البيانات على شبكة الانترنت. وبالمثل في شبكة من نوع Class B يعتبر العنوان 176.10.0.0 عنوان شبكة (Network Address) كما يتضح من الشكل ١٧–١٤ يشتمل الشكل علي عنوان شبكة من نوع Class B وتلاحظ أن جميع البتات المخصصة للمضيف تحتوي علي أصفار، ولهذا يعرف هذا العنوان بعنوان شبكة أو Network Address .

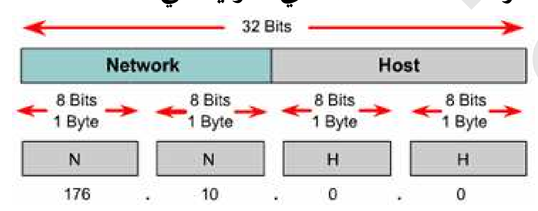


شكل ١٧–١٤ يشتمل جزء المضيف من عنوان الشبكة علي أصفار

تخصص أول ثمانيتين من عنوان شبكة **Class B** لجزء الشبكة. وتحتوي آخر ثمانيتين من العنوان علي أصفار لأنها مخصصة لرقم المضيف وتستخدم لتعريف الوحدات أو الأجهزة المتصلة بالشبكة.

ويعتبر العنوان **176.10.0.0** الذي شرحناه قبل قليل مثالاً لعنوان الشبكة أو **Network Address** . وهذا العنوان لا يمكن تخصيصه كعنوان مضيف (**Host Address**) فعنوان المضيف لأي جهاز موجود علي الشبكة **176.10.0.0** يجب أن يكون **176.10.16.1** . وفي هذه الحالة فإن أول ثمانيتين وهما "**176.10** " يقال عنهما جزء الشبكة بينما يقال عن الثمانيتين الأخيرتين وهما "**16.1**" جزء المضيف .

عندما ترغب في إرسال بيانات إلى جميع أجهزة الشبكة فسنحتاج إلي عنوان **Broadcast** "عنوان بث". كما يتضح من شكل ١٧–١٥ عندما يرسل أحد نقاط الشبكة البيانات إلي جميع الوحدات والأجهزة الموجودة على الشبكة يحدث **Broadcast** "بث". عادة يشمل عنوان **Broadcast** علي آحاد في كل الجزء المخصص للمضيف من العنوان . وذلك لأن **255** هي القيمة العشرية المكافئة للثمانية التي تحتوي علي القيمة الثنائية **11111111**.

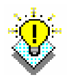


يشتمل جزء عنوان المضيف **(Host)** من عنوان الشبكة **Network Address** علي أصفار

N	N	H	H
176 .	10 .	255 .	255

يشتمل جزء عنوان المضيف من عنوان البث **Broadcast Address** علي آحاد

شكل ١٧–١٥



تذكر أن عنوان الشبكة هو الجزء من العنوان الذي يحدد أي شبكة يوجد عليها جهاز الكمبيوتر، بدلاً من تعريف جهاز الكمبيوتر المحدد . علي سبيل المثال : يعد 192.168.1.X عنوان شبكة لأجهزة الكمبيوتر ، حيث يمكن أن تتراوح X من 0 إلى 255 . ويعد عنوان البث هو العنوان الذي يمكن استخدامه لإرسال رسائل إلى كل الأجهزة على الشبكة. عادة، يعد عنوان البث أعلى رقم في الشبكة المحلية؛ وفي المثال السابق، يعد 192.168.1.255 هو عنوان البث.

عناوين IP العامة والخاصة Private and Public IP Addresses

يجب أن يعين عنوان مميز وفريد لكل جهاز موجود على الشبكة لأن تكرار العنوان لأكثر من جهاز علي نفس الشبكة يجعل من المستحيل علي الموجه أن يعيد توجيه حزمة البيانات.

عناوين IP العامة (Public) عادة تكون مميزة وفريدة، حيث لا يمكن لأي جهازين علي نفس الشبكة أن يخصص لهما نفس العنوان، وذلك لأن عناوين IP العامة معروفة وثابتة ، لأنك تحصل عليها من مزود خدمة الانترنت (Internet Service Provides (ISP.

ولكن مع تطور الانترنت أصبحت العناوين العامة بدائية . وظهرت تقنيات حديثة للعنونة مثل IPV6. أو Classless Interdomain Routing (CIDR) لحل مشاكل العناوين العامة . (سنشرح كلاً من IPV6 و CIDR بعد قليل)

كما ذكرنا من قبل ، تحتاج الشبكات العامة (Public Network) مضيف لكي تخصص عناوين IP فريدة. أما الشبكات الخاصة (Privet Network) التي لا تتصل بشبكة الانترنت، يمكنها استخدام أي عنوان مضيف طالما أن كل مضيف داخل الشبكة الخاصة مميز وفريد. في كثير من الأحيان تعمل الشبكة الخاصة بجانب الشبكة العامة.

يحتاج توصيل شبكة باستخدام عناوين خاصة بالانترنت إلي ترجمة العناوين الخاصة إلي عناوين عامة.

يقال عن عملية الترجمة هذه NAT أو Network Address Translation "ترجمة عناوين الشبكة" ويقوم الموجه بهذه العملية في العادة .

الحاجة إلي عناوين IP إضافية

لقد أصبح تقلص مساحة عناوين الإنترنت بصورة سريعة حقيقة واقعة. يعد ذلك صحيحاً لأن المصممين الأصليين للإنترنت لم يتصوروا على الإطلاق عالم توجد به أجهزة كمبيوتر شخصية؛ ولم يتخيلوا على الإطلاق أن 4.294.667.296 عنوان سوف تقترب مساحة العنوان الخاصة بها التي تبلغ 32 بت، من أن تكون مستخدمة بالكامل .

لم يتصور هؤلاء المصصمون أيضاً أنه سوف يكون هناك اتصال مباشر بين المستخدمين وبروتوكولات الإنترنت وأن المستخدمين سوف يكون عليهم توصيف عناوين IP وأقنعة الشبكة الفرعية و DNS ، وما شبه ذلك. كذلك، لم يتخيل المصصمون عالماً تتصل فيه أجهزة كمبيوتر يدوية أو هواتف خلوية بالإنترنت.

نظراً لأن الشبكة الأولية لمصصمي الإنترنت كانت غير تجارية، فإنهم لم يتخيلوا أنهم سوف يحتاجون إلى طريقة لتأمين معاملات تجارية مؤمنة. لقد كانوا يعلمون أن اتصال الشبكات كان سريعاً، ولكنهم لم يدركوا أن تردد النطاق سوف يكون قيداً على نمو الشبكة. ونظراً لأنهم لم يتصورا النمو الذي شهدته الإنترنت، فإنهم لم يدركوا أن بروتوكول الإنترنت كان قادراً على ترتيب أهمية تدفق الاتصالات لأسباب جودة الخدمة .

في ظل نظام عناوين الإنترنت التي تبلغ 32 بت الحالي والمعروف باسم IPv4، يجب أن تحدد المؤسسات فئة الشبكة التي سوف توفر عناوين IP كافية لاحتياجاتها. يمكن تعيين عناوين الفئة A القليلة المتبقية للمؤسسات التي تحتاج أكثر من 65.536 عنوان IP (حجم عناوين الفئة B)، حتى إن لم تطلب المؤسسة عناوين يقترب عددها من 16 مليون عنوان.

وبالمثل ، يتم تعيين عناوين الفئة B للمؤسسات التي تطلب أكثر من 256 عنوان IP، سواء أكانت تطلب عناوين يقترب عددها من 65.536 أم لا.

لحسن الحظ، تتوفر عناوين الفئة C للشبكات الصغيرة. على الرغم من ذلك، ضع في حسبانك أنك إذا أخذت عنواناً كاملاً من الفئة C ، سوف يكون لديك 256 عنوان، حتى إذا طلبت 20 عنواناً فقط.لحسن الحظ، هناك عدة حلول متوفرة. يتمثل الحل الأول في CIDR أو Classless Inter-Domain Routing "توجيه النطاقات الداخلية بلا

فئات" أو Network Address Translation أو NAT "ترجمة عناوين الشبكة" سوف نعود لشرح كل منهما بعد قليل.

يتمثل حل آخر (يقترب ولكنه لم يتم تنفيذه بالسرعة المطلوبة) في IPV6، أو الجيل التالي من بروتوكول IP. لبروتوكول IPV6، علي عكس IP الحالي (وهو IPV4) مساحة عناوين تبلغ 128بت (مقابل مساحة العناوين التي تبلغ 32 بت الخاصة ببروتوكول IPV4) ويتم تخطيطه بطريقة مختلفة عن IPV4. انظر الشكل التالي :

يتم تمثيل عنوان IPv4 هكذا X.X.X.X حيث تمثل كل X ثماني بتات في الرموز العشرية المنقطة (من 1 إلي 255)

بينما يتم تمثيل عنوان IPv6 هكذا X:X:X:X:X:X:X:X حيث تمثل كل X ستة عشر بت مكتوبة برموز سداسية عشرية (من 0 إلي F).

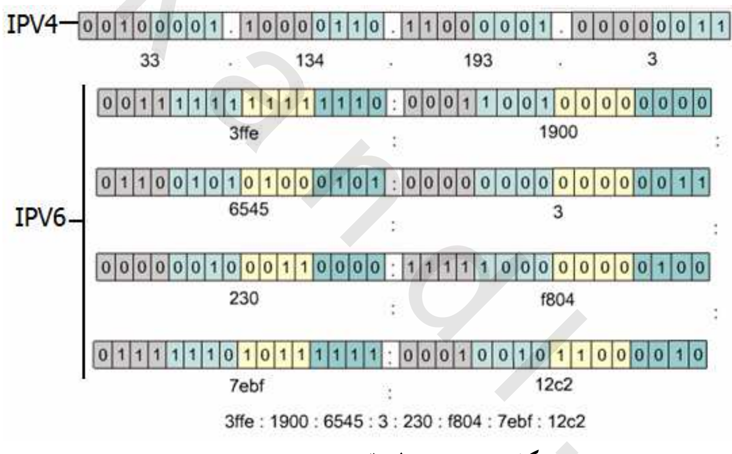
عنونة IPv6 ومقارنتها مع IPv4

تتم كتابة عناوين IPv6 بأرقام سداسية عشرية أو النظام 16. يتم استخدام الأرقام السداسية عشرية نظراً لأنه إذا تمت كتابة كل رقم يبلغ 16 بت بين النقطتين بأرقام عشرية، سوف يكون العنوان ضخم. (تذكر أن البتات الستة عشر يمكن أن تمثل أي رقم بدايةً من 0 إلي 65.536).

إذا لم تكن علي دراية بالنظام السداسي عشر راجع الفصل الثالث من هذا الكتاب ، باستخدام الرموز السداسية عشرية، من الممكن تمثيل رقم IPv6 بطريقة تقترب من الفهم هكذا FEDC:BA98:7654:3210 ، سوف يتخلص IPv6 من مشكلة مساحة العنوان التي كانت تواجه IPv4. كيف ذلك ؟ تذكر أن البتات 32 تمثل مساحة عنوان لما يزيد علي 4 بليون عنوان مختلف. لنوضح الآن إذا كانت البتات 32 تساوي 4,294,967,296 عنوان مختلف، سوف نضيف بت واحداً إضافياً (لجعل الإجمالي 33 بت) ويصبح لدينا 8,589,934,592 عنوان. اجعلها 34 بت، وسوف يصبح لديك 17,179,869,184 عنوان. استمر في مضاعفة هذا الرقم مع كل بت إضافي حتى تصل إلي 128 بت، وسوف ترى أن الرقم يستمر في الزيادة بسرعة كبيرة. إذا استمررت في مضاعفة الكمية التي تُملها

سلسلة البتات حتى تصل إلي 128 بت، سوف ينتهي بك الحال بـــ 340 بليون بليون بليون بليون عنوان. يعني ذلك أنه سوف يكون هناك ملايين العناوين لكل شخص موجود علي سطح الكرة الأرضية بفرض أن عدد سكان الأرض سيتضاعف مئات المرات عما هو عليه الآن. أي أن العناوين لن تنفذ في أي وقت قريب علي الإطلاق إذا استخدمنا IPv6.

يبلغ طول حقول IPV6 ١٦ بت (16 bits) لكل منها، وليس ٨ كما هو الحال في IPV4 ولأن كل رقم سداسي عشر يمثل ٤ أرقام بالنظام الثنائي فإن كل حقل سيحتوى على ٤ أرقام بالنظام السداسي عشر وهذا ما تراه في شكل ١٧-١٦. لكي تجعل العناوين أسهل في قراءتها يمكن حذف الأصفار الموجودة علي يسار كل حقل فمثلا يمكن كتابة حقل يحتوي علي :003 هكذا :3



شكل ١٧-١٦ الفرق بين IPv4 و IPv6

من هذا الشكل نلاحظ الآتي :

- **يتكون IPV4 من ٤ ثمانيات ثنائي كل ثمانية بها ٨ بتات مفصولة بعلامة (.)**
- **يتكون IPV6 من ١٢٨ بت تخصص أربعة أرقام بالنظام السداسي عشر لكل ١٦ بت مفصولة بعلامة (:) .**
- **الصف الأول يعبر عن عناوين IPV4 والصفوف الأخيرة تعبر عن IPV6 لأن الصفحة لا تتسع لوضع الـــ ١٢٨ بت بجانب بعضها فقد وضعنا كل ٣٢ بت في صف. ويكون مجموع الصفوف الأربعة ١٢٨ بت.**

- كتبنا تحت كل ثمانية بتات القيمة العشرية المكافئة لها في IPv4 وتحت كل ١٦ بت القيمة السداسية عشر المكافئة لها في IPv6 .

سوف يتمكن مديرو النظم ومنشئو الشبكات من الاسترخاء أيضاً ؛ حيث يقدم IPv6 إمكان توصيف تلقائي يتم فيه تضمين عنوان MAC لبطاقة الشبكة في عنوان IPv6 . يضمن هذا الترتيب عناوين فريدة ويمنع التعارض بين العناوين. كذلك، لميزتي الاكتشاف التلقائي والتوصيف التلقائي فائدة إضافية، حيث يمكن لمحطات العمل التي تستخدم برامج وأجهزة IPv6 أن توصف نفسها تلقائياً للشبكة التي يتم توصيلها بها.

مع زيادة استخدام IPv6 على نطاقٍ واسع، سوف يتم تحرير ربط الشبكات من العديد من المعوقات الفنية الحالية، وسوف ينمو بصورة كبيرة. ولن يظل إنشاء الشبكات عملية مليئة بالمخاطرة ذات منحنى تعلم شديد الانحدار.

بالإضافة إلى ذلك، سوف ترضي ميزات التوثيق والتشفير المضمنة في IPv6 العملاء الذين يخشون من أداء أعمالهم التجارية عبر الإنترنت في الوقت الحالي، وسوف يساعد أيضاً على تمكين تجارة إلكترونية مؤمنة، مما يمنح الأعمال التجارية إشارة الانطلاق.

يوضح الجدول التالي الاختلافات بين IPv4 و IPv6 .

الخاصية	IPv4	IPV6
مساحة العنوان بالبت	32	128
عدد العناوين المحتملة	2^{32} أو 4.294.967.296	2^{128}أو ^{38} 3.402823669209 من الصعب الشرح هنا، ولكن عدد العناوين في IPv6 ضخم جداً. لا تعد مساحة العنوان التي تبلغ 128 بت أكبر أربع مرات من مساحة عنوان IPV4 التي تبلغ 32 بت، ولكنها تعد أكبر منها ببليون بليون مرة أو نحو ذلك.

الخاصية	IPv4	IPV6
		باستخدام IPv6، لن تنفذ العناوين لفترة طويلة جداً.
طول الرأس ، بالبايت (يطلق عليها أيضاً ثمانيات)	20 ثُماني	40 ثُماني. لاحظ أنه على الرغم من أن مساحة العنوان تزيد في الطول عن IPv4 بأربع مرات، فإن الرأس، الذي يحتوي على معلومات توجيه حزم البيانات، يعد أكبر بمرتين فقط. يمثل ذلك استخداماً فعالاً جداً لتردد النطاق.
قابلية الامتداد	لا	نعم في هذا السياق، يقصد بقابلية الامتداد أن الخيارات التي لا يجب قراءتها بالضرورة في كل مرة يتم فيها توجيه حزم البيانات توجد في رؤوس الامتداد الموجودة بعض معلومات الرأس الجوهرية. يستغل هذا الترتيب تردد النطاق بصورة أفضل.
التشفير والتوثيق والخصوصية	لا	نعم .يتسم IPv6 بإمكانات مضمنة لتوثيق مرسل حزم البيانات وتشفير البيانات الموجودة في حزمة البيانات.

الخاصية	IPv4	IPV6
التوصيف التلقائي	لا	نعم . يتوفر في IPv6 إمكانات لتوصيف عنوان IP تلقائياً لنفسه، ويمكن أن يعمل مع شبكات لتلقي عناوين الشبكة الفريدة المناسبة.
إمكانات جودة الخدمة	لا	نعم

بالإضافة إلى الاختلافات المدرجة في الجدول السابق، يجهز IPv6 أيضاً عملية انتقال بسيطة من IPv4 إلى IPv6. توضح متطلبات المستندات التي طلبتها مؤسسة IETF أن الانتقال من IPv4 إلى IPv6 يجب أن تلبي المتطلبات الأربعة التالية :

- يجب أن يكون من الممكن ترقية شبكة IPv4 إلى شبكة IPv6 دون الحاجة إلى فعل ذلك في سيناريو الكل أو لا شيء. لذلك، يجب أن يكون IPv6 متوافقاً مع IPv4.
- يجب أن يكون من الممكن نشر الأجهزة الجديدة التي يمكنها استخدام IPv6، على الشبكة دون تغيير أي من أجهزة كمبيوتر IPv4 على الشبكة.
- عندما تتم ترقية أجهزة كمبيوتر IPv4 إلى IPv6، يجب أن تكون قادرةً على استخدام عناوين IPv4 الموجودة الخاصة بها في سياق IPv6– لا يحتاج الأمر إلى أي تغيير.
- لا يجب ألا تكون تكلفة نشر IPv6 زائدة، وتتطلب الترقية من IPv4 إلي IPv6 بعض الإعداد.

مفهوم Classless Inter-Domain Routing (CIDR) (توجيه النطاقات الداخلية غير المصنفة)

على الرغم من أن IP الحالي يدعم عدة بلايين مضيف، فإنه لم يعد كافياً. تحصل المزيد من الشركات على Class B (الفئة B) كاملة (65.536 عنوان IP) أو Class C (الفئة C) كاملة (256 عنوان IP) عندما تطلب عناوين IP أقل فعلياً من المخصص وفقاً لقواعد النطاقات الحالية. تؤدي هذه العملية بصورة سريعة إلى نقص في عناوين Class B (الفئة B) و Class C (الفئة C) المتوفرة– على الرغم من أن العديد من عناوين IP المضيفة هذه لا يتم استخدمها. كذلك، أصبح حجم Routing Tables (جداول التوجيه) في الموجهات هائلاً، مما يعني أن الإنترنت سوف تعمل بصورة أبطأ. وهذا وضع سيئ بطبيعة الحال .

يوفر (CIDR) Classless Inter-Domain Routing "توجيه النطاقات الداخلية غير المصنفة" طريقة للتحايل على قيود تخصيص عناوين IP القياسي. بصفة أساسية، يمكن هذا التوجيه دمج عناوين Class C (الفئة C)، مع التحايل على طريقة تخصيص الفئة A أو B أو C التي تُملي بوجود 16 مليون أو 65.536، أو 256 عنواناً مضيفاً، ولا شيء في الوسط (لذلك، يطلق عليها Classless (غير مصنفة). يُطلق على هذا الأسلوب– بصفة عامة– اسم Supernetting (الشبكة الفائقة)، نظراً لأنه بدلاً من تقسيم شبكة كبيرة إلي شبكات أصغر حجماً، فإنها تدمج شبكات أصغر حجماً في شبكة واحدة أكبر.

باستخدام CIDR، سوف تتمكن أية مؤسسة تجارية كانت تأخذ عنوان Class B (الفئة B) بأكمله وتترك معظمه غير مستخدم. من دمج شبكات Class C (الفئة C) بها بما يصل إلى 256 عنوان IP . أي أن CIDR يجعل استخدام عناوين IP أكثر كفاءة من تخصيصات عناوين الفئة A أو B أو C القياسية ، التي توفر 16 مليوناً و 65.000 و256 عنوان لكل فئة على التوالي.

مثال على ذلك : باستخدام CIDR، إذا كنت بحاجة إلي ألف عنوان شبكة، يمكنك الحصول على أربعة عناوين من الفئة C التي تبلغ 256 ودمجها للحصول على إجمالي يبلغ 1,024

عنوان (1024 = 4 * 256) ، بدلاً من كتابة عنوان كامل من الفئة B من العناوين التي تبلغ 65.536. لقد أصبح CIDR، أو الشبكة الفائقة، كما يطلق عليه، وسيلة لتخصيص عناوين الشبكة بكفاءة، دون إهدار كتل كبيرة من مساحة عناوين الفئة B.

ما سبب أهمية ذلك بالنسبة للشبكة؟ هناك ثلاثة أسباب:

- يستخدم CIDR مجموعة متقلصة من عناوين IP بكفاءة أكبر من تخصيص عناوين IP للفئة A أو B أو C القياسية. نظراً لأن الشبكات الحديثة تتصل بالإنترنت بصفة شائعة، فإنها تتطلب عناوين IP. كلما زادت فعالية استخدام عناوين IP، طال الوقت الذي سوف نتمكن خلاله من إضافة شبكات جديدة إلى الإنترنت.
- يمثل CIDR طبقةً إضافيةً من التعقد إلي جداول التوجيه. مع زيادة شعبية CIDR، سوف تتطلب الشبكة موجهات أكثر أو أسرع، نظراً لأن حجم جداول التوجيه أصبح على وشك الانفجار. (سوف نشرح التوجيه والموجهات في الفصل التالي)
- إذا كنت تريد استخدام CIDR، يجب أن تكون الأجهزة والمكونات الخاصة بك قادرةً على دعمه. من الأفضل الاستعداد له عن طريق التأكد من أن الموجهات الخاصة بك يمكنها دعم CIDR (اسأل الشركة المصنعة)،بالإضافة إلى بروتوكولات المدخل المختلفة. بالتأكد من أن الموجهات تدعم CIDR من البداية، سوف تتجنب سلسلة كاملة من المشكلات. حتى يتم تطبيق IPv6 (بمساحة عناوينه التي تبلغ 128بت والعدد غير المحدود تقريباً من عناوين IP) على نطاق واسع، سوف يظل CIDR جزءاً أساسياً إن لم يكن مركزياً في توجيه IP.

مفهوم NAT

في الوقت الحالي، تعد أكثر الطرق شيوعاً للتخلص من ضغط عناوين IP هي Network Address Translation (ترجمة عناوين الشبكة) أو NAT . باستخدام NAT، لا تحتاج المؤسسة إلى الكثير من عناوين الإنترنت، ولكنها تحتاج إلى عناوين للنظم التي يجب الوصول إليها من الانترنت. يترجم جهاز NAT العناوين الداخلية (التي قد تكون على مساحات شبكة خاصة) إلى عناوين إنترنت، ويعمل بصفته واجهة الإنترنت للشبكة

الداخلية.إذا كان لديك موجه كبل أو **DSL** يستخدم شبكة **192.168.1.0** لأجهزة الكمبيوتر الموجودة على جانب الداخل (غير الإنترنت) من الشبكة، يعني ذلك أن الموجه يجري عملية **NAT** . بمرور الوقت أثبتت **NAT** بالاشتراك مع النظم التأمينية أنها أسهل طريقة لمد مساحة العناوين المحدودة للإنترنت.

عناوين IP الثابتة والمتغيرة

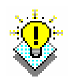
يحتاج مضيف الانترنت أن يحصل على عناوين عامة وفريدة لكي تعمل الانترنت بكفاءة. العنوان المادي أو عنوان **MAC** المخصص للمضيف هو عنوان محلي لتعريف المضيف داخل الشبكة المحلية. ولأن هذا هو عنوان الطبقة رقم ٢، فإن الموجه لا يستخدمه لتوجيه البيانات خارج شبكة **LAN**.

عناوين **IP** هي أكثر العناوين شيوعاً واستخداماً في شبكة الانترنت. هذا البروتوكول يأخذ الشكل الهرمي لكي يسمح للعناوين المستقلة بالاتصال ببعضها وبأن تتعامل كمجموعة وتسمح هذه المجموعات من العناوين بنقل البيانات داخل الانترنت. (راجع شكل ١٧–٣) يستخدم مدير الشبكة طريقتين لتعيين عناوين **IP** . الأولى ثابتة **Static** والثانية متغيرة (**Dynamic**). نوضح فيما يلي المقصود بكل منها.

عناوين IP الثابتة Static IP Addresses

تناسب عناوين **IP** الثابتة المؤسسات الصغيرة التي لا تحتاج إلي تغيير من وقت لآخر. ويتولي مدير الشبكة تعيين ومتابعة عناوين **IP** يدوياً لكل جهاز موجود علي الشبكة سواء كان وحدة تابعة أو طابعة أو وحدة خدمة. ولكن عليه أن يتأكد من عدم تكرار العناوين على الشبكة ويمكن أن يتحقق ذلك بتسجيل العناوين يدوياً ومتابعتها. وبالطبع فإن هذا الأمر يمكن تحقيق إذا كان عدد الأجهزة فليلاً .

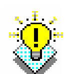
يجب أن تخصص عناوين ثابتة لوحدات الخدمة (**Server**) لكي تتعرف الوحدات التابعة علي وحدة الخدمة بسهولة. تخيل مدى الصعوبة التي يواجهها العميل للاتصال بمؤسسة إذا كانت تغير عنوانها أو رقم تليفونها كل فترة. ومن أمثلة الوحدات الأخرى التي يجب تخصيص عناوين ثابتة لها الطابعة المشتركة بين الأجهزة وجهاز الموجه.



يجب تخصيص عناوين ثابتة لوحدات الخدمة (Server) التي توفر خدمات دليل الشبكة، علي سبيل المثال: في بيئة عمل Windows 2003/2008 Server يجب توصيف Domain Controllers " وحدة التحكم في النطاق" التي تزود الشبكة ب Active Directory "الدليل النشط" باستخدام عنوان IP ثابت. ينطبق ذلك أيضاً علي خادمات Network التي توفر e Directory للشبكة .

توصيف وحدة الخدمة (Server) باستخدام إعدادات IP الثابتة

تتطلب وحدات الخدمة التي توفر خدمات مثل DNS أو DHCP أو غيرها من وحدات الخدمة الخاصة مثل وحدات الطباعة والملفات أو وحدات خدمة الويب .... وغيرها تتطلب عنوان IP ثابت.



سوف نناقش بعد قليل كل من DNS و DHCP قبل نهاية الفصل

يتم عادة توفير آلية لتوصيف جهاز كمبيوتر باستخدام عنوان IP ثابت وقناع الشبكة الفرعية بواسطة نظام تشغيل الشبكة. وعادة يتم توصيف عنوان IP وقناع الشبكة الفرعية أثناء تثبيت نظام تشغيل الشبكة Network Operating System (NOS) لكن يمكن توصيفه بعد اكتمال التثبيت (راجع نظام التشغيل الذي تستخدمه) .

إذا كانت تستخدم نظام Windows Server 2003 سيتم توصيف إعدادات TCP/IP في مربع الحوار Internet Protocol) (TCP/IP) Properties) وهذا الأخير يتم الوصول إليه من مربع Local Area Connection Properties .

عند توصيف جهاز كمبيوتر كوحدة خدمة (Server) سوف تحتاج لتزويده بمعلومات أكثر من مجرد عنوان IP وقناع الشبكة الفرعية حيث يؤدي توصيف وحدة خدمة باستخدام توصيف TCP/IP غير مكتمل إلي مشكلات في الاتصال بين وحدة الخدمة وباقي الشبكة. سوف تحتاج لتزويده بالمعلومات الآتية :

- عنوان IP ثابت وقناع الشبكة الفرعية

- المدخل الافتراضي لوحدة الخدمة وهو واجهة الموجه المتصلة بالمقطع الذي توجد عليه وحدة الخدمة.
- عنوان IP لوحدة خدمة DNS الأساسية المستخدمة لتحليل الأسماء بواسطة وحدة الخدمة.

عناوين IP المتغيرة

أفضل خيار لعنونة الوحدات التابعة للشبكة هو استخدام بروتوكول Dynamic Host Configuration Protocol (DHCP) "بروتوكول توصيف المضيف الديناميكي" .
حيث يستخدم DHCP لتوصيف وحدة تابعة لشبكة باستخدام عنوان IP وقناع شبكة فرعية ومعلومات توصيف TCP/IP أخري

ولكن ما هو DHCP ؟

يسمح لك DHCP بتعيين عنوان IP ديناميكيا لأجهزة كمبيوتر الشبكة وغيرها من الأجهزة بدون حاجة لأن يعد مدير الشبكة ملفاً لكل جهاز. وتوفر لك معظم نظم تشغيل الشبكات خدمة DHCP للتعرف علي DHCP تابع الشرح التالي.

توفير DHCP علي الشبكة

لاشك أن عملية توصيف جهاز كمبيوتر ووحدات تابعة علي شبكة بعناصر مثل عنوان IP افتراضي وقناع شبكة فرعية، وعنوان مدخل افتراضي، وعنوان خادم DNS، عملية تقود إلي احتمال الوقوع في الخطأ. وهنا تبرز أهمية DHCP حيث أنه يتولي تعيين عناوين IP تلقائياً ، وبالتالي يخفف الكثير من العمل الذي يشتمل عليه التعيين اليدوي لعناوين IP.
وبالتالي يعد استخدام DHCP أكثر الطرق توفيراً للوقت لتعيين عناوين IP وأقنعة الشبكة الفرعية وغيرها من معلومات توصيف TCP/IP للوحدات التابعة للشبكة.

يعني ذلك أنك سوف تضطر إلي توصيف وحدة خدمة DHCP (DHCP Server) علي الشبكة. قد تتطلب الشبكات الكبيرة وخاصة تلك التي يتم تقسيمها إلي شبكات فرعية أكثر من وحدة خدمة DHCP علي كل شبكة فرعية.

يجب أن تعلم أن جميع أنظمة تشغيل الشبكات الأساسية بما في ذلك Windows Server

2003/2008 أو Linux/Unix أو Novell Netware توفر خدمة DHCP بصفتها جزءاً من نظم تشغيل الشبكات الخاصة بها. وهذا يتيح لك توصيف DHCP في أي بيئة نظام تشغيل شبكات .

عادة توفر نظم التشغيل واجهة رسومية تسمح لك بتوصيف جهاز الكمبيوتر بصفته وحدة DHCP تابعة باستخدام عنوان IP ثابت.

توفر وحدة خدمة DHCP نطاق عناوين IP (وقناع الشبكة الفرعية الذي يجب استخدامه) للوحدات التابعة الخاصة بها اعتماداً علي المجال الذي يوصفه المدير علي وحدة خدمة DHCP. يعد المجال هو نطاق العناوين الذي سوف يتم تعيينه لوحدات DHCP التابعة علي الشبكة . جدير بالذكر أنه بإمكانك توصيف مجال يحتوي علي مخزن عناوين IP بالكامل. ويمكنك بعد ذلك استبعاد عناوين لتعيينها بصورة ثابتة لوحدات خدمة أو أجهزة أخري موجودة علي الشبكة (مثلاً خادمات DHCP أو أجهزة الموجه Router) بالإضافة إلي ذلك يمكنك حجز عنوان IP لجهاز معين علي الشبكة مثل استخدام عنوان IP للطابعة .

استخدام DNS علي الشبكة

DNS اختصار لعبارة Domain Name System "نظام أسماء النطاق أو المجال" . إذا كنت تستخدم TCP/IP علي الشبكة سوف تحتاج إلي وحدة خدمة DNS (DNS Server) لمعالجة تحليل الأسماء علي الشبكة. الشبكات الصغيرة يمكنها أن تستخدم DNS التي يوفرها مزود خدمة الانترنت. توفر نظم تشغيل الشبكات الأساسية مثل Windows Server 2003/2008 و LINUX/UNIX و NetWare دعماً لــ DNS . ويعد فهم كيفية عمل DNS ضرورة بالنسبة لأي مدير شبكة.

لقد تم تطوير DNS في الأساس من أجل الانترنت ، توفر خادمات DNS تحليل عنوان IP علي شبكة الانترنت، وفي الواقع أنت تستخدم DNS في كل مرة تتصل فيها بموقع Web عندما تتصل مثلاً بالموقع www.msn.com يتم تحليل هذا الاسم بواسطة خادمات DNS علي الشبكة بمساعدة خادمات DNS علي الانترنت ويتم إعادة عنوان IP الفعلي

لموقع **Web** الذي ترغب في الانتقال إليه بواسطة برنامج مستعرض الويب.

ملخص الفصل

تناولنا في هذا الفصل مفاهيم غاية في الأهمية. شرحنا كيف تتعرف أجهزة الشبكة علي بعضها، وذلك من خلال فهم عنونة **IP** وفئات العناوين وأقنعة الشبكة، شرحنا كذلك مستقبل عناوين **IP** وكيف نتغلب علي مشكلة مساحة العنونة ومقارنة عنونة **IPv4** مع عناوين **IPv6**، وشرحنا أيضا كيفية تعيين عناوين **IP** الثابتة، وكيفية استخدام بروتوكول **DHCP** لتعيين العناوين ديناميكياً .

تدريبات

١. ما هو الفرق بين عنوان **IP** وعنوان **MAC** ؟

٢. أكمل العبارات التالية بواحدة مما بين الأقواس (**IPv4 – IPv6**)

أ – تحتل عناوين .... **32Bit** مكتوبة بالنظام العشري ومفصولة بنقطة بين كل ثمانية والتي تليها.

ب – يبلغ طول حقول .... ١٦بت لكل منها.

جـ – يبلغ طول حقول .... ٨ بت لكل منها

د – تحتل عناوين .... **128Bit** ومكتوبة بالنظام السداسي عشر ومفصولة بنقطتين فوق بعضهما بين كل ستة عشر بت .

هـ – تقدم ...... إمكان توصيف تلقائي يتم فيه تضمين عنوان **MAC** لبطاقة الشبكة في عنوان **IP**.

و – يبلغ عدد عناوين .... **4.294.667.296**.

٣. إلي أي فئة ينتمي العنوان التالي : **131.15.253.219**

أ. **D**
ب. **A**
ج. **B**
د. **C**

٤. فئة عناوين **IP** التي تقبل أكبر عدد من المضيفين (الأجهزة).

أ. B
ب. C
ج. A

٥. ما هو نوع العناوين اللازم استخدامه لكي لا يكون الجهاز مرئياً علي الانترنت؟
٦. أوجد عدد الأجهزة التي يمكن توصيلها في أي شبكة من فئة A؟
٧. ما هو مجال العناوين الممكن استخدامها في الشبكات من فئة B؟
٨. ضع علامة (✓) أمام الإجابة الصحيحة وعلامة (✗) أمام الإجابة الخاطئة .

أ. يؤدي استخدام CIDR إلي إهدار كتل كبيرة من عناوين IP. ( )

ب. CIDR يجعل استخدام عناوين IP أكثر كفاءة من تخصيصات عناوين Class A أو Class B القياسية . ( )

ج. فكرة CIDR هي تقسيم الشبكة الكبيرة إلي شبكات فرعية أصغر حجماً ، وليس دمج شبكات أصغر حجماً في شبكة واحدة أكبر. ( )

د. جاءت فكرة CIDR للتغلب علي مشكلة محدودية عناوين IPv4 . ( )

هـ . مفهوم NAT واحد من الطرق المستخدمة لمد مساحة العناوين المحدودة بالانترنت. ( )

٩. أكمل بواحدة مما بين الأقواس

أ- تناسب عناوين IP الثابتة (وحدة الخدمة والطابعات – الأجهزة المضيفة)

ب-يقوم (DHCP – NAT – CIDR) بتعيين عناوين IP ديناميكياً لأجهزة كمبيوتر الشبكة.

١٠. يخص عناوين IP : 191.253.10.4 أي من عناوين فئات IP التالية :

أ. A
ب. B
جـ. C
د. D



بروتوكول الإنترنت أو **Internet Protocol** والمعروف اختصاراً باسم **IP**، يعتبر هو بروتوكول التوجيه الأساسي المستخدم داخل شبكة الإنترنت، حيث تُستخدم عناوين **IP** فى توجيه حزم البيانات من أحد المصادر (المرسل) إلى أحد الأهداف (المستقبل) من خلال أفضل مسار متاح . يجب أن تكون قد انتهيت من دراسة الفصل السابق لكي تفهم هذا الفصل. بالانتهاء من هذا الفصل ستتعرف علي:

- البروتوكولات الموجهة والبروتوكولات القابلة للتوجيه
- كيفية نقل حزم البيانات علي الشبكة
- التسليم بالاتصال والتسليم بدون اتصال
- عملية التوجيه ووظائف الموجه
- الفرق بين التوجيه والتحويل
- تنسيق جداول التوجيه وبنائها.
- عرض الاستخدامات المختلفة لبروتوكولات التوجيه

مقدمة

يمكن تعريف الموجه **(Router)** بأنه جهاز يقوم بمعالجة وتمرير حزم البيانات داخل الشبكة الواحدة أو بين شبكات **LAN** منفصلة ويتم إرسال البيانات من مصادرها إلى وجهاتها فى أسرع طريق ممكن. يعمل الموجه عند طبقة الشبكة (**Network**) وهى الطبقة الثالثة فى نموذج **OSI** الذى مر بنا فى الفصل الرابع .

فى حالة الشبكة الواحدة، تتجه حزم البيانات من الجهاز المرسل إلى الجهاز الوجهة (المستقبل) دون أية وسائط. أما إذا كان عنوان الوجهة لحزمة البيانات خارج الشبكة المحلية، سيتم إرسالها إلى الموجة (الذى يعرفه الجهاز المرسل بصفته البوابة الافتراضية أو المدخل الافتراضي **Default Gateway**) بدون معالجتها. عندما يتلقى الموجه حزمة بيانات موجهة لمكان خارج الشبكة المحلية، سوف يقوم الموجه بإرسال حزمة البيانات إلى النقطة التالية.

وللتوضيح نقول . ترسل الموجهات حزم البيانات وفقا للموجهات المتوفرة بين الشبكات وتحاول تحديد أقصر مسار توجيه ممكن فى أى وقت محدد. كيف يتم ذلك؟ يوجد داخل الموجه (وهو جهاز صغير به معالج قوى جدا) توجد مجموعة بيانات تسمى **Routing Tables** أو "جداول التوجيه". يتم تحديث هذه الجداول بواسطة بروتوكولات توجيه يطلق على أحدها **Routing Information Protocol (RIP)** أو "برتوكول توجيه المعلومات" وعلى الثاني **Open Shortest Path first (OSPF)** "فتح أقصر مسار أولا". (سنتعرض لشرح كلاً من **RIP** و **OSPF** بعد قليل)

ويقوم أى من البروتوكولين بتمرير البيانات بصفة مستمرة بين الموجهات للتأكد أن كل الموجهات لديها أحدث البيانات فيما تعلق بمسارات التوجه المتوفرة.

كيف يتم توجيه البيانات

تحتوى جداول التوجيه على جميع مسارات التوجيه الممكنة، ويستعين الموجه بجداول التوجيه لتحديد ما إذا كان لديه مسار توجيه إلى عنوان وجهة معين أو لا. إذن كل ما يفعله الموجه

هو إعادة إرسال حزم البيانات إلى وجهاها. ويحاول الموجه فعل ذلك بأفضل طريقة كيف ذلك؟

فى كل مرة يتم توجيه حزمة البيانات بين موجه وآخر يزيد رقم فى حزمة البيانات يطلق عليه عدد الوثبات أو العداد إلى عدد من المرات محددة سلفا (مثلا يسمح لبروتوكول RIP بعدد ١٦ وثبة بين المصدر والوجهة). يتم تجاهل حزمة البيانات إذا وصل عدد الوثبات إلي العدد المحدد سلفاً ، باعتبار أن الموجه حاول ١٦ مرة ولم يفلح فى تسليمها إلى عنوان الوجهة.

كانت هذه المقدمة مدخل لتوضيح فكرة الموجهات وكيفية توجه البيانات. في الحقيقة تحتاج مسألة توجيه البيانات الكثير من التفصيل نوضحها فيما يلي.

البروتوكولات الموجّهة والبروتوكولات القابلة للتوجيه

البروتوكول عبارة عن مجموعة من القواعد التى تحدد طريقة اتصال أجهزة الكمبيوتر المختلفة مع بعضها البعض من خلال الشبكات، حيث تتصل أجهزة الكمبيوتر مع بعضها البعض عن طريق تبادل رسائل البيانات. ولقبول هذه الرسائل والتعامل معها، يجب أن تحتوى هذه البروتوكولات على مجموعة من القواعد التى تحدد تفسير الرسائل المختلفة. ومن أمثل ذلك، الرسائل المستخدمة فى تحقيق الاتصال مع الأجهزة البعيدة ورسائل البريد الإلكتروني والملفات المنقولة عبر الشبكة.

ويقوم البروتوكول بوصف ما يلى:

- التنسيق المناسب للرسالة.
- الطريقة التى تستخدمها أجهزة الكمبيوتر فى تبادل الرسائل فى أنشطة محددة.

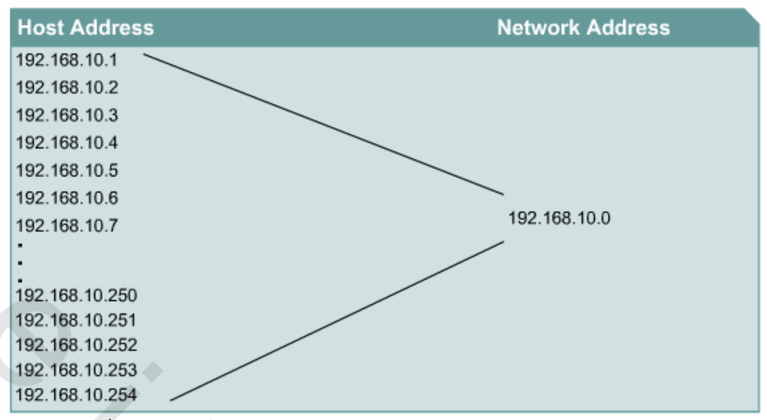
ويتيح البروتوكول الموجَّه للموجِّه **Router** دفع البيانات بين الأطراف الموجودة داخل شبكات مختلفة، حيث يجب أن يوفر البروتوكول القادر على التوجيه غالباً رقم شبكة ورقم مضيف لكل جهاز موجود بالشبكة. وتتطلب بعض البروتوكولات رقم الشبكة فقط كما فى البروتوكول **IPX**، حيث يستخدم هذا النوع من البروتوكولات عنوان **MAC** الخاص

بالجهاز المضيف كرقم لهذا المضيف. بينما تتطلب بعض البروتوكولات الأخرى كالبروتوكول الشهير **IP** عنواناً واحداً فقط يحتوى جزء منه على رقم الشبكة بينما يحتوى الجزء الآخر على رقم الجهاز المضيف، إلا أن هذه البروتوكولات تحتاج إلى قناع شبكة **Network Mask** لتمييز الرقمين عن بعضهما، حيث يتم الحصول على عنوان الشبكة عن طريق الجمع المنطقى (باستخدام المعامل **AND**) لعنوان **IP** مع قناع الشبكة.

ولعل السبب فى استخدام قناع الشبكة هو القدرة على معاملة مجموعات من عناوين **IP** المتتالية كما لو كانت وحدة واحدة. فبدون هذا التجميع، لاضطررنا إلى توجيه كل جهاز مضيف بشكل مستقل، وهو ما يستحيل فى عالم الواقع نظراً لوجود عدد هائل جداً من الأجهزة المضيفة داخل شبكة الإنترنت.

تحتوى الشبكة على عنوان **IP** للجهاز المضيف وعنوان شبكة، حيث نحتاج إلى العنوانين معاً للحصول على شبكة موجَّهة. ويستخدم قناع الشبكة فى فصل أجزاء الشبكة والجهاز المضيف. كما تقوم عملية الجمع المنطقى باستخدام المعامل **AND** بتوليد رقم شبكة نستطيع من خلاله تحديد كل واجهة على حده، حيث يجب توجيه البيانات إلى هذه الواجهة للوصول إلى الشبكة المطلوبة.

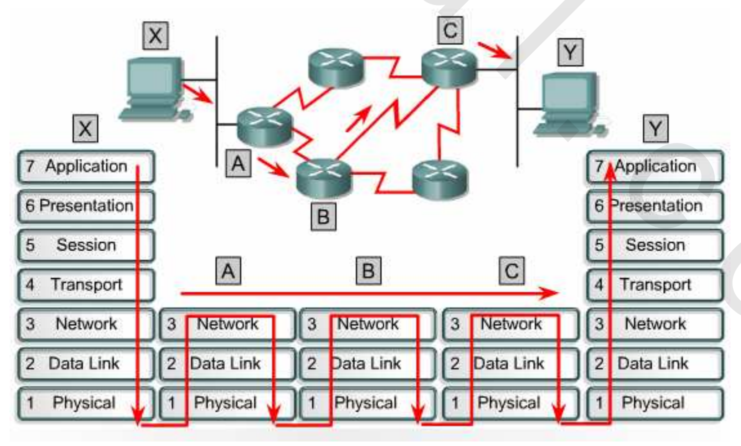
نستطيع تمثيل العناوين الموجودة فى المدى من **192.168.10.1** إلى **192.168.10.254** (أى ٢٥٤ عنواناً) بعنوان الشبكة **192.168.10.0**، وهذا يتيح نقل البيانات لأيٍ من هذه الأجهزة المضيفة عن طريق تحديد رقم الشبكة، حيث تحتاج جداول التوجيه فى هذه الحالة إلى تسجيل عنوان واحد فقط وهو العنوان **192.168.10.0** بدلاً من تسجيل ٢٥٤ عنواناً. (انظر شكل ١٨-١)



شكل ١٨-١يستخدم عنوان الشبكة **192.168.10.0** للإشارة إلي ٢٥٤ عنواناً للمضيفين

كيفية نقل حزم البيانات عبر الشبكة.

عند نقل حزمة البيانات عبر الإنترنت إلى الجهاز الهدف (الجهاز المستقبل) ، يتم حذف أجزاء الرأس والذيل بإطار الطبقة الثانية **(Data Link Layer)** مع استبدالها بكل عنصر من عناصر الطبقة الثالثة **(Network Layer)**، وذلك لأن وحدات بيانات (إطارات) الطبقة الثانية تستخدم للعنونة المحلية فقط، بينما تستخدم وحدات بيانات (حزم) الطبقة الثالثة فى العنونة الكاملة من البداية وحتى النهاية. (شكل ١٨-٢)



شكل ١٨- ٢ يقوم كل موجه بتزويد خدماته لتدعيم وظائف الطبقة العليا.

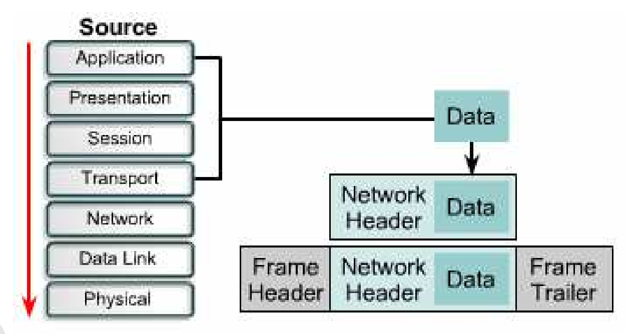
وقد تم تصميم إطارات الطبقة الثانية للعمل داخل مجال بث معين بعنوان **MAC** المعرف

داخل الجهاز. وتتضمن أنواع إطارات الطبقة الثانية الأخرى ارتباطات تسلسل **PPP** واتصالات تتابع الإطارات، والتي تستَخدم مخططات عنونة مختلفة للطبقة الثانية. وبغض النظر عن نوع نظام العنونة المستخدم بالطبقة الثانية، يتم تصميم الإطارات للعمل داخل مجال البث الخاص بالطبقة الثانية. وعند إرسال البيانات إلى جهاز موجود بالطبقة الثالثة، تتغير على الفور البيانات الموجودة بالطبقة الثانية.

وبمجرد استقبال الموجِّه **Router** لأحد الإطارات، يتم على الفور استخلاص عنوان **MAC** الخاص بالجهاز الهدف واختباره للتعرف على ما إذا كان الإطار معنون إلى الموجِّه مباشرةً أم أنه بث عام، وفى الحالتين يتم قبول الإطار، وإلا يتم تجاهل الإطار بالكلية.

وفى حالة قبول الإطار، يتم استخلاص بيانات **CRC** والتى توجد بذيل الإطار، حيث يتم استخدام هذه البيانات فى التأكد من عدم وجود أى أخطاء ببيانات هذا الإطار.

فإذا فشل الاختبار، يتم تجاهل الإطار كليةً. أما إذا تم الاختبار بنجاح، فيتم على الفور حذف بيانات الرأس والذيل الموجودة بالإطار وتمرير الحزمة الناتجة إلى الطبقة الثالثة **(Network Layer)**، وحينئذٍ يتم اختبار الحزمة الممرَّرة لمعرفة ما إذا كانت متجهة إلى الموجِّه نفسه أم إلى جهاز آخر على الشبكة. فإذا توافق عنوان **IP** مع أحد المنافذ المعرَّفة بالموجِه، يتم حذف رأس الطبقة الثالثة وتمرير البيانات الناتجة إلى الطبقة الرابعة **(Transport Layer)**. أما إذا كانت الحزمة موجَّهة إلى جهاز آخر على الشبكة، فيتم فى هذه الحالة مقارنة عنوان **IP** الخاص بالهدف مع محتويات جدول التوجيه **Routing Table**. فإذا وُجد توافق أو احتوى الجدول على اتجاه افتراضى، فسيتم توجيه حزمة البيانات إلى الوجهة المحدَّدة فى جدول التوجيه، وفى هذه الحالة يتم إضافة قيمة **CRC** جديدة إلى ذيل الإطار، كما يتم إضافة رأس الإطار المناسبة إلى حزمة البيانات، وحينئذٍ يتم بث الإطار إلى المجال التالى ليستكمل رحلته إلى الهدف النهائى. شكل ١٨–٣



شكل ١٨–٣ تقوم طبقة النقل **Transport** بتجزئة وترقيم وإضافة أخطاء المراجعة إلي رسائل البريد الالكتروني. يتم إضافة عناوين طبقة الشبكة لكل من المصدر والوجهة إلي مخطط البيانات.

التسليم بالاتصال والتسليم بدون الاتصال

يوجد نوعين من أنظمة تسليم البيانات، التسليم بالاتصال والتسليم بدون اتصال، وهما الطريقتان المستخدمتان فى تسليم البيانات داخل الشبكة.

تستخدم معظم خدمات الشبكات نظام التسليم عديم الاتصال أو ما يطلق عليه **Connectionless Delivery System**. فربما تأخذ الحزم المختلفة مسارات مختلفة للمرور داخل الشبكة، حيث يتم إعادة نمذجة هذه الحزم بعد وصولها إلى أهدافها. وفى النظم عديمة الاتصال، لا يتم إنشاء اتصال بين المرسل والمستقبل قبل إرسال حزمة البيانات، وهو ما يتشابه إلى حدٍ كبير مع النظام البريدى، حيث لا يلزم أن يكون المستقبل موجوداً لتتحدد إمكانية استقبال أحد الخطابات قبل إرسال الخطاب بالفعل. كما أن المرسل لا يعرف إذا كان الخطاب قد وصل بالفعل إلى المستلم أم لا.

أما فى الأنظمة المبنية على الاتصال **Connection-oriented Systems**، فيتم إنشاء الاتصال بين المرسل والمستقبل قبل إجراء عملية نقل البيانات. وخير مثال على ذلك نظام التليفون، حيث يقوم المتصل بإجراء عملية الاتصال التى لا تتم إلا بتحقيق الاتصال أولاً مع الجانب الآخر.

ويتم عادةً تسمية عمليات الشبكات عديمة الاتصال بالعمليات المبنيَّة على تحويل الحزم أو **Packed-switched processes**. فعند مرور حزم البيانات من المصدر إلى الهدف،

يمكن تحويل هذه الحزم إلى مسارات مختلفة، كما أنها لا تصل بالضرورة فى نفس ترتيب إرسالها، حيث تحتوى كل حزمة بيانات على التعليمات اللازمة لوضعها فى الترتيب المناسب بمجرد وصولها للهدف، مثل عنوان الهدف وترتيب الحزمة داخل الرسالة، وبالتالى يتم إعادة نمذجة حزم البيانات المختلفة لتظهر بالترتيب الصحيح لدى الهدف. ويتم تحديد المسار الذى تسلكه كل حزمة من خلال عدد من المعايير، والتى ربما تختلف من حزمة بيانات إلى أخرى.

أما عمليات الشبكة المبنيَّة على الاتصال، فيتم عادةً تسميتها بالعمليات المبنيَّة على تحويل الدوائر أو **Circuit-switched processes**، والتى يتم فيها بدايةً إنشاء الاتصال بين المصدر والهدف ثم تبدأ بعد ذلك عملية نقل البيانات، حيث يتم نقل جميع الحزم بنفس ترتيبها عبر نفس الدائرة فى عملية تدفق مستمرة من البداية وحتى النهاية.

وتعتبر شبكة الإنترنت شبكة عملاقة عديمة الاتصال، يتم فيها احتواء الغالبية العظمى من حزم البيانات من خلال البروتوكول **IP**. أما البروتوكول **TCP** فيقوم بدوره بإضافة الخدمات المبنيَّة على الاتصال بالطبقة الرابعة **(Transport Layer)** إلى اتصالات **IP** عديمة الاتصال (الغير مبنية على الاتصال).

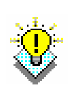
عملية التوجيه ووظائف الموجه (Router)

تعتبر عملية التوجيه إحدى وظائف طبقة **OSI** الثالثة **(OSI Layer 3)**، وهي طبقة **Network**، وهى عبارة عن مخطط تنظيمى هرمى يتيح تجميع العناوين المستقلة مع بعضها البعض فى قالب واحد، حيث يتم معاملة هذه العناوين كوحدة واحدة إلي أن تحتاج إلى عنوان الهدف لتوصيل البيانات إليه، وبهذا تختص عملية التوجيه بتوفير المسار الأمثل لنقل البيانات من جهاز ما إلى جهاز آخر. ويعتبر الموجِّه **Router** الجهاز الأساسي الذى يقوم بأداء هذه المهمة.

فإذا أراد جهاز معين إرسال بيانات إلي جهاز آخر، فإن مسار البيانات يتحدد بواسطة بروتوكولات التوجيه التي يستخدمها الموجه.

وحقيقةً فإن للموجه وظيفتين أساسيتين وهما:

- تعتنى الموجِّهات بجداول التوجيه وتتأكد من معرفة الموجِّهات الأخرى للتغييرات التى تحدث فى تركيبة الشبكة، حيث تُستخدم بروتوكولات التوجيه فى تحقيق الاتصال بين بيانات الشبكة وبقية الموجهات.
- عند وصول حزم البيانات إلى أى واجهة (Interface) ، يجب أن يستخدم الموجِّه نفس جدول التوجيه لتحديد المكان الذى يقوم بإرسال البيانات إليه، حيث يقوم الموجِّه بتحويل حزم البيانات إلى الواجهة المناسبة ثم إضافة بيانات الإطار الخاصة بهذه الواجهة وأخيراً إرسال الإطار.



الواجهة Interface عبارة عن عنوان بطاقة الشبكة الذي يجب أن يستخدمه الجهاز لإرسال رزم البيانات إلي النظام المحدد.

والموجِّه Router عبارة عن جهاز بطبقة الشبكة يستخدم وحدة قياس أو أكثر لتحديد المسار الأمثل لإرسال البيانات عبر الشبكة، حيث تُستخدم وحدات القياس هذه فى تمييز بعض الموجهات عن البعض الآخر. كما تستخدم الموجهات توليفات مختلفة من القياسات لتحديد أفضل مسار للبيانات.

وتقوم الموجهات بربط أجزاء الشبكة الواحدة أو ربط أكثر من شبكة مع بعضها البعض، حيث تقوم بتمرير إطارات البيانات بين الشبكات بالاستعانة ببيانات الطبقة الثالثة Layer 3. كما تقوم الموجِّهات باتخاذ القرارات المثلى حول أفضل المسارات المستخدمة فى نقل البيانات ثم توجيه حزم البيانات إلى منفذ الخرج المناسب لتغليفها وإرسالها بعد ذلك، حيث تتم عملية تغليف البيانات وفكها مرةً أخرى فى كل مرة يتم فيها نقل حزمة البيانات من خلال الموجِّه والذى يجب أن يقوم بدوره بفك تغليف إطار بيانات الطبقة الثانية حتى يتمكن من اختبار عنوان الطبقة الثالثة. تتضمن عملية نقل البيانات من جهاز إلى آخر تغليف البيانات وفكها فى جميع طبقات OSI السبعة، حيث تقوم عملية التغليف بتقسيم البيانات إلى أجزاء صغيرة ثم إضافة بيانات الرأس والذيل المناسبة ثم إرسال البيانات، بينما تقوم عملية فك التغليف على الجانب الآخر بحذف بيانات الرأس والذيل ثم تجميع الأجزاء الصغيرة مع بعضها البعض مرةً أخرى.

ويركز هذا المنهج على أكثر البروتوكولات القابلة للتوجيه وهو البروتوكول **IP**. وهناك بالطبع بروتوكولات أخرى كالبروتوكول **IPX/SPX** والبروتوكول **AppleTalk** حيث تدعم هذه البروتوكولات الطبقة الثالثة **Layer 3**، وهو ما لا تدعمه البروتوكولات الأخرى الغير قابلة للتوجيه مثل البروتوكول **NetBEUI** وهو أحد البروتوكولات الصغيرة والسريعة التى تعمل بكفاءة عالية عند نقل الإطارات داخل جزء واحد فقط.

الفرق بين التوجيه Routing والتحويل Switching

سنقوم فيما يلي بمقارنة التوجيه والتحويل، حيث يقوم كلاهما بأداء نفس الوظيفة تقريباً. الفرق الأساسى أن المحولات **Switches** تعمل بالطبقة الثانية **Layer 2** من نموذج **OSI** وهي الطبقة **Data Link** بينما تعمل الموجهات بالطبقة الثالثة **Layer 3** وهي طبقة **Network**، وهذا يعنى أن كلاهما يستخدم بيانات مختلفة لإرسال البيانات من المصدر إلى الهدف.

ويمكن مقارنة العلاقة بين الموجهات والمحولات بمكالمات التليفون المحلية والدولية. فعند إجراء مكالمة تليفونية محلية، يتم استخدام محول (مفتاح) محلى يتعامل فقط مع المكالمات المحلية ولا يمكنه بالطبع التعامل مع جميع المكالمات الموجودة بالعالم. فإذا استقبل المحول طلب مكالمة خارج نطاقه المحلى، يقوم على الفور بتحويل المكالمة إلى محول أعلى يجيد التعامل مع هذا النوع من المكالمات ويعرف أكواد المناطق الخارجية، ومن ثم يقوم هذا المحول بدوره بتحويل المكالمة إلى محول محلى فى محيط التليفون المطلوب.

ويقوم الموجه بوظيفة مشابهة إلى حد كبير للمحول الأعلى فى مثال المكالمات التليفونية الذى ذكرناه منذ قليل. ويقوم محول الطبقة الثانية ببناء جدوله باستخدام عناوين **MAC**. وحينما يكون لدى الجهاز المضيف بيانات لعنوان **IP** خارجى، يقوم هذا الجهاز بإرسال البيانات لأقرب موجِّه، حيث يطلق على هذا الموجِّه فى هذه الحالة البوابة الافتراضية لهذا الجهاز المضيف أو **Default Gateway**، كما يستخدم الجهاز المضيف عنوان **MAC** الخاص بالموجِّه كعنوان **MAC** خاص بالهدف.

ويقوم المحول **Switch** بربط الأجزاء الصغيرة التى تنتمى لنفس الشبكة. وفى حالة الأجهزة

المضيفة الغير محلية، يقوم المحول بتوجيه الإطار إلى الموجِّه بناءً على عنوان **MAC** الخاص بالهدف. ويقوم الموجِّه باختبار عنوان الهدف الموجود بالطبقة الثالثة لحزمة البيانات لاتخاذ قرار توجيه الحزمة، ويتعرف الجهاز المضيف **X** على عنوان **IP** الخاص بالموجِّه نظراً لاحتواء تركيب **IP** الخاص بالجهاز المضيف على عنوان **IP** الخاص بالبوابة الافتراضية.

وكما أن المحول يحتوى على جدول من عناوين **MAC** المعروفة، يحتوى الموجِّه على جدول من عناوين **IP** وهو الذى يسمى بجدول التوجيه. ولا يتم تنظيم عناوين **MAC** بطريقة منطقية، بينما يتم تنظيم عناوين **IP** تنظيماً هرمياً. ويستطيع المحول احتواء عدد محدود من عناوين **MAC** الغير منظمة، بينما تحتاج الموجِّهات إلى نظام عناوين منظَّم يستطيع تجميع العناوين المتشابهة مع بعضها البعض وبالتالى معاملتها كوحدة واحدة داخل الشبكة حتى تصل البيانات إلى الهدف المطلوب.

ولولا تنظيم عناوين **IP** فى شكل هرمى منظَّم، لما عملت شبكة الإنترنت. وهذا ما يمكن تشبيهه بمكتبة تحتوى على ملايين الأوراق المطبوعة المتناثرة فى كل مكان بالمكتبة، وهو ما يعنى أن هذه الأوراق عديمة الفائدة لصعوبة الوصول إلى ورقة معينة بداخلها. فمن الصعب الوصول إلى ورقة معيَّنة داخل ملايين الأوراق. فإذا قمنا بتنظيم هذه الأوراق داخل مجموعة من الكتب مع وضع محتويات كل كتاب فى فهرس مستقل ببداية الكتاب، لكان الوصول إلى أى ورقة غاية فى السهولة.

فرق آخر بين الموجهات والمحولات وهو أن الموجهات تقدم مستوي أعلي من السرية ويمكنها التحكم في تردد النطاق (**Bandwidth**) أكثر من المحولات (انظر شكل ١٨-٤) تعتمد مقارنة السرعة والسرية علي إمكانيات الجهاز

Features		Router	Switch
Speed	السرعة	Slower	Faster
OSI Layer	طبقة OSI	Layer 3	Layer 2
Addressing used	العناوين المستخدمة	IP	MAC
Broadcasts	البث	Blocks	Forwards
Security	السرية	Higher	Lower

شكل ١٨-٤ مقارنة بين الموجه والمحول

تحديد المسار الصحيح للبيانات

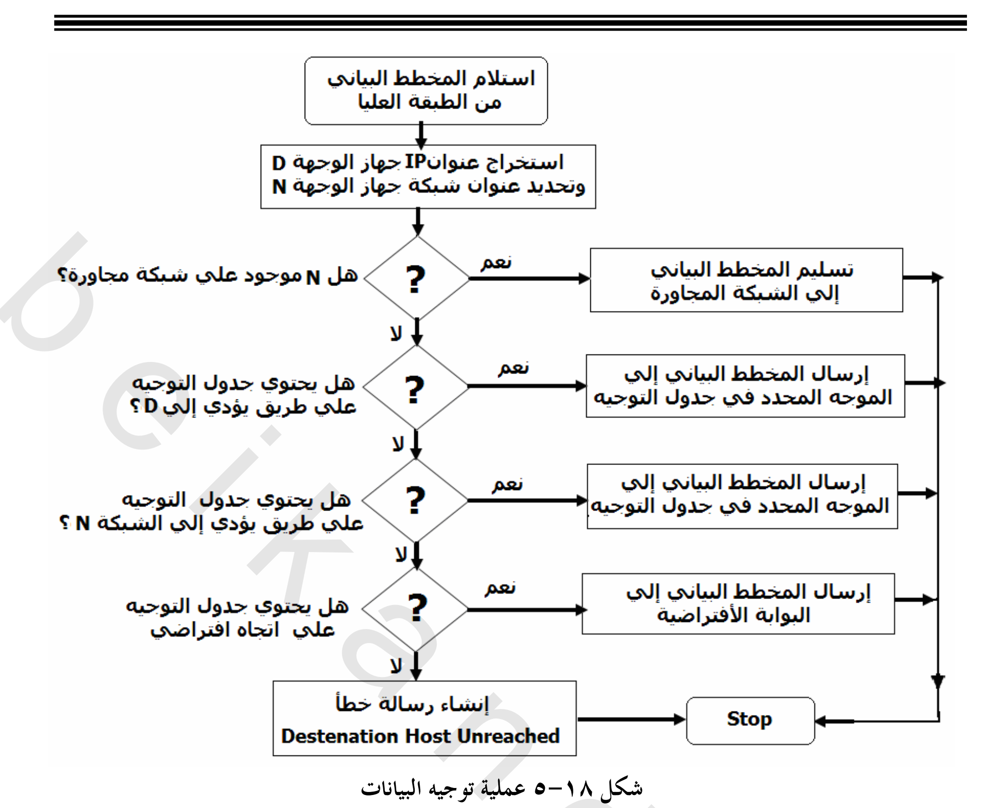
تتم عملية تحديد المسار فى طبقة الشبكة **Network Layer**، ويستخدم الموجِّه هذه العملية فى مقارنة عنوان الهدف مع الاتجاهات المتاحة فى جدول التوجيه المصاحب ثم اختيار المسار الأمثل، حيث تتعرف الموجَّهات على الاتجاهات المتاحة من خلال عملية توجيه ديناميكية أو عملية توجيه ساكنة. فالتوجيهات الساكنة هى التى يقوم فيها مسئول الشبكة بتهيئة الموجِّه بطريقة يدوية، أما التوجيهات الديناميكية فهى الاتجاهات التى يتم تعليمها من خلال الموجهات الأخرى باستخدام أحد بروتوكولات التوجيه. (سنشرح بعد قليل التوجيه الساكن والتوجيه الديناميكي)

ويستخدم الموجِّه عملية تحديد المسار فى تحديد المنفذ الذى يتم إرسال حزمة البيانات من خلاله كى تصل إلى هدفها، وهو ما يطلق عليه "توجيه حزمة البيانات"، كما يطلق على كل موجِّه يصادف حزمة البيانات فى رحلتها من المصدر إلى الهدف "قفزة" أو **Hop**. ويمكن مقارنة عملية تحديد المسار بشخص يقود سيارة من مكانٍ ما داخل مدينة إلى مكانٍ آخر. هذا الشخص لديه خارطة بشوارع المدينة المختلفة والتى يمكنه من خلالها التعرف على الطرق والشوارع التى يمكن أن يسلكها للوصول إلى المكان الهدف، تماماً كما يحتوى الموجِّه على جدول توجيه. وينتقل السائق من تقاطع إلى آخر تماماً كما تنتقل حزمة البيانات من موجِّه إلى آخر فى كل قفزة. وعند أى تقاطع، يستطيع السائق الذهاب يساراً أو يميناً أو الاستمرار إلى الأمام، وهى نفس طريقة تحديد الموجِّه للمنفذ الذى يتم إرسال حزمة البيانات من خلاله.

وتعتمد قرارات السائق للسير فى اتجاه معيَّن على عدة عوامل منها الكثافة المرورية فى الاتجاهات المختلفة ونطاق السرعة وعدد الممرات والإشارات وما إذا كان الطريق مغلقاً فى العادة، وغيرها من العوامل الأخرى. وأحياناً يكون من الأسرع أن نسلك الطريق الأطول إذا كانت كثافته المرورية أقل من الطريق الأقصر. وبنفس الطريقة، تأخذ الموجِّهات قرارها بناءً على حمل خط الشبكة وعرض الموجه وزمن التأخير والتكلفة وغيرها من العوامل المؤثرة الأخرى.

لنوضح الآن كيف تتم عملية اختيار المسار من قبل البروتوكول **IP** المسئول عن عملية التوجيه وهذا من خلال استخدامه للإجراءات المبينة في الشكل ١٨-٥ من أجل تحديد مسار كل حزمة يتم توجيهها والذي يتم علي الخطوات التالية:

- يقوم الموجِّه بمقارنة عنوان **IP** الخاص بالحزمة التى قام باستقبالها مع جداول **IP** الموجودة لديه.
- يتم الحصول على عنوان الهدف من حزمة البيانات.
- يتم تطبيق القناع الموجود بأول عنصر بجدول التوجيه على عنوان الهدف.
- يتم مقارنة الهدف المقنَّع مع العنصر الموجود بجدول التوجيه.
- فى حالة حدوث توافق، يتم توجيه حزمة البيانات إلى المنفذ المصاحب لهذا العنصر داخل الجدول.
- فى حالة عدم وجود توافق، يتم اختبار العنصر التالى داخل جدول التوجيه.
- إذا لم تتوافق حزمة البيانات مع أيٍ من العناصر الموجودة بجدول التوجيه (عناوين الشبكة والشبكة الفرعية ، يقوم الموجه باختبار وجود بوابة افتراضية **Default Gateway** معرَّفة مسبقاً.
- إذا كان هناك بوابة افتراضية، يتم توجيه حزمة البيانات إلى المنفذ المصاحب. والبوابة الافتراضية هي البوابة التي تم تهيئتها بواسطة مسئول الشبكة لاستخدامها فى حالة عدم وجود توافق بجدول التوجيه.
- فى حالة عدم وجود بوابة افتراضية، يتم تجاهل حزمة البيانات، وإعادة الرسالة إلى مصدرها مرةً أخرى لتوضيح عدم إمكانية الوصول إلى الهدف.



شكل ١٨–٥ عملية توجيه البيانات

جداول التوجيه Routing Table

تستخدم الموجهات بروتوكولات التوجيه لإنشاء جداول التوجيه **Routing Tables** والتعامل مع قيمها المختلفة، وهذا يساعد فى عملية تحديد المسار التى ذكرناها منذ قليل، حيث تقوم بروتوكولات التوجيه بتعبئة جداول التوجيه ببيانات التوجيه المختلفة، وهى البيانات التى تختلف باختلاف البروتوكول المستخدم. وتحتوى جداول التوجيه على البيانات الضرورية لإرسال حزم البيانات عبر الشبكات المتصلة.

وتعتبر جداول التوجيه من المعلومات المهمة التي يعتمد عليها الموجه. فمن خلال هذه الجداول يصنع الموجه قراراته في توجيه البيانات.

ويتم بناء جداول التوجيه إما يدوياً أو بصفة أوتوماتيكية . عملية إنشاء جداول التوجيه يدوياً ممكنة علي الشبكات الصغيرة وهذا ما يدعي التوجيه الساكن (**Static Routing**).

لكن علي الشبكات الكبيرة تعتبر هذه العملية شاقة جداً وفي بعض الحالات تكون غير ممكنة .

تتم عملية إنشاء الجداول بصفة أوتوماتيكية في الشبكات الكبيرة ومن خلال بروتوكولات مختصة تستخدمها الموجهات لتبادل المعلومات عن نفسها وعن الشبكات المحيطة بها . من بين هذه البروتوكولات نذكر RIP و OSPF (سنشرح بروتوكولات التوجيه في البند التالي).

إذا أراد نظام إرسال رزمة إلي كمبيوتر علي الشبكة المحلية، تأمره جداول التوجيه أن يعنون الرزمة إلي ذلك النظام، وهذا ما يسمي بالتوجيه المباشر. في هذه الحالة الحقل Destination IP Address في ترويسة IP والحقل Destination Address في ترويسة إطار طبقة ربط البيانات يشيران إلي نفس الجهاز. أما إذا كانت وجهة الرزمة علي شبكة أخري فتأمر جداول التوجيه أن تعنون الرزمة إلي موجه آخر. في هذه الحالة ، يشير الحقل Destination IP Address إلي عنوان IP جهاز الوجهة ويشير الحقل Destination Address إلي العنوان المادي للموجه الموجود علي الشبكة المحلية، وتسمي هذه العملية التوجيه غير المباشر.

تنسيق جداول التوجيه

جدول التوجيه هو عبارة عن قائمة تحتوي علي عناوين شبكات وعناوين الموجهات التي يستطيع النظام استخدامها للوصول إلي تلك الشبكات، يوضح الجدول التالي شكل جدول التوجيه.

Network Address	Net Mask	Gateway Address	Interface	Metric
0.0.0.0	0.0.0.0	192.168.16.99	192.168.16.1	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.16.0	255.255.255.0	192.168.16.1	192.168.16.1	1
192.168.16.1	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.16.255	255.255.255.255	192.168.16.1	192.168.16.1	1
244.0.0.0	224.0.0.0	192.168.16.1	192.168.16.1	1
255.255.255.255	255.255.255.255	192.168.16.1	192.168.16.1	1

وفيما يلي نوضح وظائف الأعمدة المختلفة في الجدول السابق

- ***Network Address** (عنوان الشبكة)*

يشير هذا العمود إلي عنوان الشبكة أو الجهاز المضيف الذي تشير إليه معلومات التوجيه المذكورة في باقي الأعمدة.

- ***Net Mask** (قناع الشبكة)*

يحدد هذا العمود قناع الشبكة الفرعية للقيمة في العمود **Network Address**. من خلال هذا القناع نستطيع التعرف علي عنوان الشبكة، وعنوان الشبكة الفرعية وعنوان المضيف.

- ***Gateway Address** (عنوان البوابة)*

يدل هذا العمود عن عنوان الموجه الذي يجب أن يستخدمه النظام لإرسال البيانات إلي الشبكة أو الجهاز المذكور في العمود **Network Address** .

- ***Interface** (الواجهة)*

يدل هذا العمود عن عنوان بطاقة الشبكة الذي يجب أن يستخدمه الجهاز لإرسال الرزم إلي النظام المحدد في العمود **Gateway Address**.

- ***Metric** (القياس)*

يمثل هذا العمود قيمة تمكن النظام من مقارنة الفعالية النسبية للمسارات التي يمكن سلوكها للوصول إلي نفس الوجهة.

يحتوي الجدول السابق علي مداخل معيارية لمحطة عمل عادية لا تعمل كموجة. قد تكون جداول التوجيه المستخدمة في الموجهات أعقد بكثير من جداول محطات العمل. تحتوي الجداول في هذه الحالة علي مداخل لكل الشبكات التي يتصل معها الموجه، بالإضافة إلي مداخل قد تكون سجلت يدوياً وأخري سجلت ديناميكياً عن طريق بروتوكولات التوجيه، وتتصل الموجِّهات مع بعضها البعض للحفاظ على جداول التوجيه الخاصة بها من خلال نقل رسائل تحديث التوجيه، حيث يقوم بعض بروتوكولات التوجيه بنقل رسائل التحديث بطريقة دورية، بينما يقوم البعض الآخر بإرسال هذه الرسائل عند وجود تعديلات فى هيكل الشبكة. كما يقوم بعض البروتوكولات بإرسال جدول التوجيه كاملاً مع كل رسالة

تحديث، بينما يقوم البعض الآخر بإرسال التوجيهات التى حدث لها تغيير فقط.

بناء جداول التوجيه

توجد وسيلتان لبناء جداول التوجيه، وسيلة التوجيه الساكن وطريقة التوجيه الديناميكي. التوجيه الساكن هو عملية إنشاء مداخل جدول التوجيه بصفة يدوية. أما التوجيه الديناميكي فهو عملية إنشاء مداخل جدول التوجيه بصفة تلقائية من خلال بروتوكولات توجيه متخصصة تعمل علي الموجهات. من بين البروتوكولات الشائعة في هذا المجال نذكر:

- **Routing Information Protocol (RIP)** "بروتوكول معلومات التوجيه"
- **Open Shortest Path First (OSPF)** " بروتوكول فتح أقصر مسار أولاً"

تستخدم الموجهات هذين البروتوكولين لتبادل رسائل تحتوي علي معلومات التوجيه مع الموجهات المجاورة لها.

يستخدم التوجيه الساكن في الشبكات الصغيرة، أما التوجيه الديناميكي فيستخدم في الشبكة الضخمة التي تحدث فيها تغييرات في المسارات بصفة مستمرة.

إنشاء مسارات ساكنة

لإنشاء مداخل أو مسارات ساكنة في جدول التوجيه نستخدم أداة مساعدة تأتي مع طقم البروتوكولات **TCP/IP** والتي يتم تشغيلها من سطر الأوامر. تستخدم أنظمة تشغيل **Windows** المختلفة برنامج اسمه **Route** والتي تكون صيغته بالشكل التالي:

Route [-p] [Command [Destination][Mask Netmask][Gateway] [Metric metric] [IF interface]

حيث :

- **p-** : يمكن هذا العامل من إنشاء مدخل أو مسار دائم في جدول التوجيه.
- **Command** : معامل يدل علي وظيفة الأمر.
- **Destination** : يدل هذا المعامل علي عنوان الشبكة أو الجهاز الذي نريد الوصول إليه.
- **Mask Network** : يحدد **Netmask** قيمة قناع الشبكة الفرعية الذي سيتم تطبيقه

علي العنوان المحدد في **Destination** .

- **Gateway** : معامل يدل علي عنوان الموجه اللازم استخدامه للوصول إلي الشبكة المحددة في **Destination** .
- **Metric metric** : يحتوي المعامل **Metric** علي قيمة تدل علي الفعالية النسبية للمسار.
- **IF Interface** : يدل المعامل **Interface** علي عنوان محول الشبكة الذي يجب أن يستخدمه النظام للوصول إلي الموجه المحدد في **Gateway** .

ويأخذ المعامل **Command** إحدى القيم التالية :

- **PRINT** : عرض محتويات جدول التوجيه.
- **ADD** : إنشاء مدخل جديد في جدول التوجيه.
- **DELETE** : حذف مدخل موجود في جدول التوجيه.
- **CHANGE** : تعديل عوامل مدخل في جدول التوجيه.

مثال

لتوضيح كيف يستطيع الموجه **A** توجيه الرزم إلي الموجه **B** بعد إضافة مسار ساكن إلي جدول التوجيه في الموجه **A** ، نفذ الأمر التالي من سطر الأوامر في الموجه **A**:

Route ADD 192.168.6.0 MASK 255.255.255.0 192.168.4.9 IF 192.168.4.1 METRIC 1

حيث أن وظائف هذه العوامل في هذا الأمر كما يلي :

- **ADD** : إنشاء مدخل جديد في جدول التوجيه.
- **192.168.6.0** : عنوان الشبكة التي نريد الوصول إليها من خلال الموجه **B**.
- **MASK 255.255.255.0** : قيمة قناع الشبكة الفرعية الذي يطبق علي عنوان الوجهة.
- **192.168.4.9** : عنوان محول الشبكة في الموجه **B** والمتصل بالشبكة المحلية **A**.
- **IF 192.168.4.1** : عنوان محول الشبكة في الموجه **A** والذي يجب أن يستخدمه النظام للوصول إلي الموجه **B** .

- **METRIC 1** : يدل أنه يوجد واحد (فقرة واحدة) بين الموجه **A** والشبكة **192.168.6.0** .

يتسبب تنفيذ الأمر السابق في إنشاء مدخل جديد في جدول توجيه الموجه **A** . يعني هذا أنه إذا استلم الموجه **A** بيانات يريد إرسالها إلي أي جهاز في الشبكة ذات عنوان **192.168.6.0** ، فعليه أن يرسلها إلي الموجه ذي عنوان **192.168.4.9** مستخدماً محول الشبكة ذا عنوان **192.168.4.1** في الموجه **A**.

بروتوكولات التوجيه *Routing Protocols*

تستخدم الموجهات مجموعة من البروتوكولات لتحديد الطريقة المناسبة لتوجيه حزم البيانات تسمى هذه البروتوكولات "بروتوكولات المداخل" أو **Gateways Protocols**. وتعد هذه البروتوكولات أفراداً فى مجموعة بروتوكولات **TCP/IP** التى تستخدمها الموجهات لتحديد أفضل مسار توجيه لحزم البيانات.

تنقسم بروتوكولات الموجه أو بروتوكولات المداخل إلى قسمين :

القسم الأول : بروتوكولات المدخل الداخلي وتشتمل على اثنين من البروتوكولات الأول يطلق عليه **Routing Information Protocol** وتختصر **RIP** ويمكن ترجمتها "بروتوكول توجيه المعلومات" والثاني **Open Shortest Path first** وتختصر **OSPF** ويمكن ترجمتها " فتح أقصر مسار أولا".

القسم الثانى : بروتوكولات المدخل الخارجى وتشتمل أيضا على اثنين من البروتوكولات . الأول " **Border Gateway Protocol** وتختصر **BGP** ويمكن ترجمتها "بروتوكول مدخل الحدود" والثانى **Exterior Gateway Protocol** وتختصر **EGP** ويمكن ترجمتها "بروتوكول المدخل الخارجي" لا تنزعج من هذه الأسماء. فسوف تتعود عليها بعد قليل وفيما يلى توضيح للبروتوكولات التي يستخدمها الموجه .

البروتوكول IGP *والبروتوكول* EGP

النظام المستقل **Autonomous System** عبارة عن شبكة أو مجموعة من الشبكات الواقعة تحت تحكم مسئول ، حيث يتكون النظام من مجموعة من الموجِّهات التى تكون صورة لتوجيه العالم الخارجى.

ويوجد عائلتان من بروتوكولات التوجيه وهما **Interior Gateway Protocols** "بروتوكولات المدخل الداخلي" **(IGPs)** و **Exterior Gateway Protocols** **(EGPs)** "بروتوكولات المدخل الخارجي" .

ومن بروتوكولات **IGPs** التى تقوم بتوجيه البيانات ما يلى:

- البروتوكول **Routing Information Protocol RIP** "بروتوكول توجيه المعلومات" والبروتوكول **RIPv2**
- البروتوكول **IGRP** : (**Interior Gateway Routing Protocol**)
- البروتوكول **EIGRP**: (**Enhanced Interior Gateway Routing Protocol**)
- البروتوكول **OSPF** : **Open Shortest Path First** "فتح أقصر مسار أولاً"
- البروتوكول **(IS-IS)** : **Intermediate System-to-Intermediate System protocol** .

أما بروتوكولات **Exterior Gateway Protocols (EGPs)** "بروتوكولات المدخل الخارجي" فتقوم بتوجيه البيانات بين الأنظمة المستقلة وهذه يتم استخدامها لتوجيه حزم البيانات إلي خارج الشبكة المحلية كما فى حالة البروتوكول **BGP**. (**Border Gateway Protocol**) "بروتوكول مدخل الحدود"

سنتعرف فيما يلي على بروتوكول حالة الارتباط **Link state** وبروتوكول التوجيه بالمسافة **Distance vector**. ثم نعود لشرح بروتوكول **BGP**

استخدام البروتوكول Link state والبروتوكول Distance vector

يتم تصنيف بروتوكولات التوجيه كما ذكرنا منذ قليل إلى صنفين أساسيين وهما بروتوكولات **IGPs** وهي التي يتم استخدامها لتوجيه شبكة داخلية، وبروتوكولات **EGPs** وهي التي يتم استخدامها لتوجيه حزم البيانات خارج الشبكة المحلية. كما يتم تقسيم بروتوكولات **IGPs** إلى بروتوكولات حالة الارتباط **Link state** وبروتوكولات التوجيه بالمسافة **Distance vector**. نتعرف فيما يلي على نوعى التوجيه ووقت استخدام كلا منهما.

التوجيه بالمسافة **Distance Vector** : يعتمد التوجيه بالمسافة على تحديد المسافة والاتجاه إلى أى ارتباط داخل الشبكة. هذه المسافة ربما تكون عدد القفزات إلى الارتباط، كما تقوم الموجِّهات التى تستخدم ألجورثمات التوجيه بالمسافة **Distance vector** بإرسال كل أو جزء من عناصر جدول التوجيه إلى الموجِّهات المجاورة على فترات دورية، وهذا يحدث حتى فى عدم وجود أى تغييرات بالشبكة. وباستقبال تحديث التوجيه، يستطيع الموجِّه التأكد من جميع التوجيهات المعروفة وإجراء التغييرات على جدول التوجيه المصاحب، حيث يطلق على هذه العملية "التوجيه بالإطلاق" **Routing by rumor**.

ومن أمثلة بروتوكولات التوجيه بالمسافة **Distance vector** ما يلى:

- البروتوكول **Routing Information Protocol (RIP)** "بروتوكول توجيه المعلومات" وهو أكثر بروتوكولات **IGP** استخداماً بالإنترنت ويحتوى على قياس واحد فقط وهو عدد القفزات **Hop count** . يمكن لـــ **RIP** توجيه حزم البيانات بحد أقصي ٦ مرات.

يعتبر البروتوكول **RIP** أحد بروتوكولات التوجيه بالمسافة **Distance-vector** والتى تستخدم عدد القفزات كقياس فى تحديد اتجاه ومسافة أى ارتباط داخل الشبكة. فإذا كان هناك أكثر من مسار للهدف، يقوم البروتوكول **RIP** باختيار المسار الذى يحتوى على أقل عدد من القفزات، إلا أنه لا يختار دائماً

المسار الأسرع نظراً لعدم احتوائه على أى قياسات غير قياس عدد القفزات كما ذكرنا منذ قليل. كما أنه لا يستطيع توجيه حزمة بيانات تحتوى على أكثر من ١٥ قفزة. كما أن الإصدار الأول من بروتوكول **RIP** أو **RIPv1** يحتاج إلى استخدام جميع أجهزة الشبكة لنفس قناع الشبكة الفرعية **Subnet Mask** وذلك لأنه لا يقوم بتضمين بيانات قناع الشبكة الفرعية فى تحديثات التوجيه، وهو ما يعرف بالتوجيه الطبقى **Classful Routing**.

أما الإصدار الثانى من البروتوكول والمعروف باسم **RIP Version 2 (RIPv2)** فيدعم عملية التوجيه المسبق، كما يقوم بإرسال بيانات قناع الشبكة الفرعية فى عمليات تحديث التوجيه، وهو ما يسمى بالتوجيه غير الطبقى **Classless Routing** والذى يتم فيه تخصيص أقنعة مختلفة لكل شبكة فرعية داخل نفس الشبكة وهو ما يسمى تقنيع الشبكات الفرعية متغيرة الطول أو **Variable-length subnet masking (VLSM)**.

- البروتوكول **Interior Gateway Routing Protocol (IGRP)** "بروتوكول توجيه بوابة المدخل الداخلي. هذا البروتوكول عبارة عن بروتوكول توجيه يعمل بتوجيه المسافة **Distance-vector** تم تصميمه من قِبَل **Cisco**. وقد تم تطوير هذا النوع من البروتوكولات للتغلب على المشاكل المصاحبة للتوجيه داخل الشبكات الكبيرة التى تخرج عن نطاق البروتوكولات الأخرى كالبروتوكول **RIP** على سبيل المثال. ويستطيع البروتوكول **IGRP** اختيار أسرع مسار من المسارات المتاحة بالاستعانة بقياساته المختلفة والتى تتضمن زمن التأخير وعرض الموجه والحمل والفاعلية. كما يحتوى البروتوكول **IGRP** أيضاً على عدد أكبر من مدى القفزات مقارنةً بالبروتوكول **RIP**، كما يستخدم التوجيه الطبقى فقط.
- البروتوكول **Enhanced IGRP (EIGRP)** يعتبر الإصدار المتقدم من بروتوكول **IGRP** ويحتوى على العديد من سمات بروتوكول التوجيه بحالة

الارتباط Link state، لذا يسمى بالبروتوكول متوازن التهجين أو Balanced-hybrid Protocol إلا أنه فى حقيقة الأمر بروتوكول توجيه بالمسافة يحتوي علي كفاءة تشغيل عالية لتدعيمه سرعات التقاء عالية وعرض موجه علوي منخفض.

***بروتوكولات حالة الارتباط* Link State**

أما بروتوكولات التوجيه بحالة الارتباط Link State على الجانب الآخر، فقد تم تصميمها خصيصاً لتخطى القيود الموجودة ببروتوكولات التوجيه بالمسافة، فهى تتميز باستجابتها السريعة لتغيرات الشبكة كما أنها تقوم بإرسال تنويهات التحديث فقط عند حدوث أى تغيير داخل الشبكة، كما تقوم هذه البروتوكولات بإرسال تحديثات دورية تسمى بتحديثات حالة الارتباط أو Link-state refreshes وذلك على فترات زمنية سريعة (كل ٣٠ دقيقة مثلاً).

وعند حدوث أى تغيير فى التوجيه أو الارتباط، يقوم الجهاز الذى اكتشف التغيير بإنشاء إعلان بحالة الارتباط يسمى Link-state advertisement (LSA) لهذا الارتباط. ومن ثم يتم إرسال LSA إلى جميع الأجهزة المجاورة، حيث يأخذ كل جهاز توجيه نسخة من LSA ويقوم بتحديث قاعدة بيانات ارتباطاته ثم تمرير LSA إلى جميع الأجهزة المجاورة. وهذا الفيض من LSAs مطلوب للتأكد من إنشاء جميع أجهزة التوجيه لقواعد البيانات التى تعكس بدقة تركيب الشبكة قبل تحديث جداول توجيهها المصاحبة.

وتستخدم ألجورثمات حالة الارتباط قواعد بياناها فى إنشاء عناصر جدول التوجيه التى تفضل المسار الأقصر طولاً. ومن أمثلة بروتوكولات حالة الارتباط البروتوكول Shortest Path First (OSPF) فهو عبارة عن بروتوكول توجيه من نوع حالة الارتباط Link-state تم تطويره بواسطة Internet Engineering Task Force (IETF) فى سنة ١٩٨٨، وذلك لتلبية احتياجات الشبكات المتداخلة كبيرة الحجم التى لا يستطيع البروتوكول RIP التعامل معها.

والبروتوكول **Intermediate System-to-Intermediate System (IS-IS)** عبارة عن بروتوكول توجيه من نوع حالة الارتباط أيضاً يستخدم مع البروتوكولات الموجَّهة غير البروتوكول **IP**. كما يوجد بروتوكول **IS-IS** المتكامل والذى يدعم عدة بروتوكولات موجَّهة تتضمن البروتوكول **IP** أيضاً.

البروتوكول Border Gateway Protocol (BGP) " بروتوكول مدخل الحدود "

هو أحد أمثلة البروتوكول **External Gateway Protocol (EGP)**، حيث يقوم بتبادل بيانات التوجيه بين الأنظمة المستقلة **Autonomous Systems** مع ضمان الاختيار الحر للمسار المناسب. ويعتبر بروتوكول **BGP** بروتوكول التوجيه الرئيسى المستخدم لدى معظم الشركات ومزودى الخدمة على شبكة الإنترنت. وعلى عكس بروتوكولات **IGPs** (مثل البروتوكول **RIP** والبروتوكول **OSPF** والبروتوكول **EIGRP**)، لا يستخدم البروتوكول **BGP** قياسات مثل عدد القفزات وعرض الموجه أو زمن التأخير، وإنما يأخذ قرارات التوجيه تبعاً لسياسات الشبكة أو القواعد التى تستخدم صفات المسار الخاصة بالبروتوكول **BGP**.

ملخص الفصل

شرحنا في هذا الفصل البروتوكولات الموجهّة والبروتوكولات القابلة للتوجيه. ثم شرحنا كيفية نقل حزم البيانات علي الشبكة وتناولنا الوظائف التي يقوم بها الموجه لضمان توصيل حزم البيانات إلي وجهتها الصحيحة. تعرضنا كذلك لكيفية تنسيق جداول التوجيه وبنائها وأخيرا شرحنا الاستخدامات المختلفة لبروتوكولات التوجيه.

تدريبات

١. تمتلك شركة الكمبيوترات المحدودة وحدة خدمة تستخدمها جميع إدارات الشركة ويخصص لكل إدارة من إدارات الحسابات وحدة خدمة مستقلة و بصفتك مدير

للشركة و تريد أن تتأكد من تحقق السرية بين إدارات البيع و إدارات المحاسبة، ماذا ستفعل من أجل ذلك :

أ. سنقوم بتثبيت Hub.

ب. سنقوم بتثبيت Switch.

ج. سنقوم بتثبيت Router.

د. سنقوم بتثبيت Bridge.

٢. ماذا يفعل RARP .

أ. يحول عناوين IP إلى عناوين MAC .

ب. يحول عناوين MAC إلى عناوين IP.

ج. يحول عناوين IP إلى عناوين IPX.

د. يحول عنوان شبكة إلى DLCI.

٣. ماذا تريد لتوجيه جيد .

٤. اختر مما يلي بروتوكول Link State .

أ. RARP
ب. IGRP
ج. NLSP
د. OSPF
هـ. ELGRP

٥. أكمل الإجابة الصحيحة بواحدة من بين القوسين (المحول Switch – الموجة Router)

أ. يعمل بالطبقة الثانية من نموذج OSI وهي طبقة Data Link ....

ب. يعمل بالطبقة الثالثة من نموذج OSI وهي طبقة Network...............

ج. يقوم ببناء جدول باستخدام عناوين MAC لأنه يحتوي علي عناوين MAC...........

د. يحتوي علي جدول من عناوين IP وهو الذي يسمي جدول التوجيه ....

هـ. يستطيع احتواء عدد محدود من عناوين MAC...............

و. يحتاج إلي نظام عناوين منظم يستطيع تجميع العناوين المتشابهة مع بعضها البعض...........

ز. يقدم مستوي أعلي من السرية ويتحكم أكثر في تردد النطاق............

٦. في جدول التوجيه في Windows، ما هو العمود الذي يحتوي علي عنوان الموجه الذي يجب استخدامه للوصول إلي شبكة أو مضيف معين ؟

أ – Network Destination .

ب – Netmask

جـ – Gateway

د – Interface

٧. ماذا يفعل الموجه عندما لا يحصل ضمن جداول التوجيه علي مدخل لشبكة أو مضيف معين؟

٨. في أنظمة Windows ، ما هو الأمر الذي نستخدمه لعرض محتويات جداول التوجيه؟

٩. في أنظمة Windows ، ما هو الأمر الذي نستخدمه لإضافة مدخل في جداول التوجيه؟

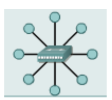
١٠. في جدول التوجيه في Windows ، ما هي قيمة العمود Network Address في مدخل البوابة الافتراضية ؟

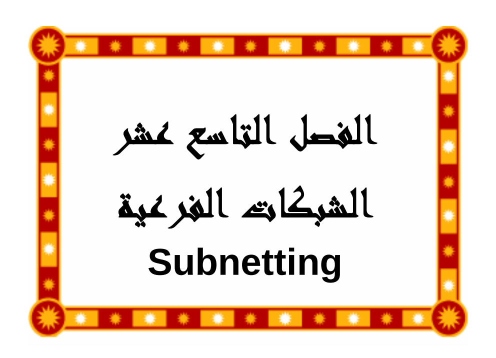
أ – 127.0.0.0

ب – 0.0.0.0

جـ – 224.0.0.0

د – 255.255.255.255





للتعامل مع مجموعة محددة من عناوين IP بكفاءة عالية، يمكن تقسيم جميع التصنيفات إلى شبكات فرعية صغيرة، سنتعرف في هذا الفصل على أهمية التشبيك الفرعي Subnetting والحاجة إلى استخدامه. يجب أن تنتهي من دراسة الفصل السابق لكي تفهم هذا الفصل لأننا نعتبر أن هذا الفصل امتداد للفصل السابق. بالانتهاء من هذا الفصل ستتعرف علي :

- كيفية عمل التشبيك الفرعي وأهميته
- تأسيس قناع الشبكة الفرعية
- تطبيق قناع الشبكة الفرعية
- حساب عنوان شبكة فرعية باستخدام ADDing

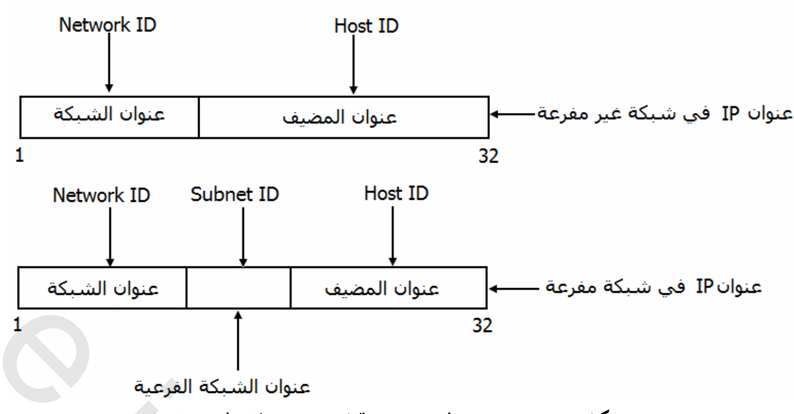
للتعامل مع مجموعة محددة من عناوين IP بكفاءة عالية، يمكن تقسيم جميع التصنيفات إلي شبكات فرعية صغيرة. يمكن أن تعطي تصنيفات IP مدي من الأجهزة المضيفة من 256 إلي 16.8 مليون مضيف (Host). سنتعرف في هذا الفصل علي أهمية التشبيك الفرعي Subnetting والحاجة إلي استخدامه.

كيفية عمل التشبيك الفرعى وأهميته

إذا كان لدينا عنوان من فئة A مثلاً، فإنه من المستحيل تكوين من خلاله شبكة محلية تحتوي علي أكثر من ستة عشر مليون مضيف (16777214) أو جهاز. حتي ولو حصل ذلك فستصبح عيوب الشبكة أكبر من مزاياها. وغالباً ما تظهر هذه العيوب في صعوبة إدارة وصيانة الشبكة.

زيادة علي ذلك سيحدث تدهور في أداء الشبكة والذي يتمثل في بطء عملية الاتصال بين الأجهزة. غالباً ما يكون هذا البطء ناتجاً عن عملية تبادل الرسائل كالبث أو التبليغ (Broadcast) . فمن خلال هذه الملاحظة نري أنه من الضروري إجراء عملية تفريع للشبكة (Sunbnetting)، لأن هذه العملية تؤدي إلي تحسين أداء الشبكة والتي غالباً ما تتمثل في ارتفاع سرعة إرسال واستقبال البيانات لأن نطاقات التصادم Collision domain ، وتبادل الرسائل والبلاغات يصبح محدداً بفرع من فروع الشبكة والذي غالباً ما يكون فيه عدد الأجهزة أقل بكثير مما هو عليه في الشبكة الجامعة غير المفرعة.

في حالة تفريع الشبكة يعني استخدام قناع تفريع غير افتراضي سيتكون عنوان IP من ثلاثة أجزاء وهي مميز الشبكة Net ID ، مميز الشبكة الفرعية Subnet ID ومميز المضيف Host ID. يبين الشكل التالي تنسيق لعنوان IP قبل وبعد عملية التفريع. (انظر شكل ١٩-١)



شكل ١٩-١ تنسيق لعنوان IP قبل وبعد عملية التجزئة

لإنشاء هيكل الشبكة الفرعية، يجب إعادة تخصيص البتس (Bits) الخاصة بالجهاز المضيف بالبتس الخاصة بالشبكة، وهو ما يطلق عليه أحياناً **Lending bits** "اقتراض البتس"، حيث تتم هذه العملية بدءاً من البت الموجودة بأقصى يسار الجهاز المضيف.

وتشمل عناوين الشبكة الفرعية الأجزاء **Class A** و**Class B** و**Class C** من الشبكة إلى جانب حقل الشبكة الفرعية **Subnet Field** وحقل الجهاز المضيف **Host**، حيث يتم إنشاء الحقلين الأخيرين من جزء الجهاز المضيف الأساسى لأكبر عنوان **IP**. وهذا يحدث بإعادة تخصيص البتس من جزء الجهاز المضيف إلى جزء الشبكة داخل العنوان مما يعطى مرونة شديدة لمسئول الشبكة فى عنونة الأجهزة المختلفة المتصلة بالشبكة. (انظر شكل ١٩-٢ أ و ب و جـ)

في هذا الشكل يشير حرف **N** إلي كلمة **Network** وحرف **H** إلي كلمة **Host** ، أما **sN** فمعناها **Subnet** .

Class C network address 192.168.10.0
11000000.10101000.00001010.00000000 N . N . N . H
11000000.10101000.00001010.00000000 N . N . N . SN H

شكل ١٩-٢ أ في هذا المثال تم تخصيص ٣ بتات (3 Bits) لتصميم الشبكة الفرعية

Class B network address 147.10.0.0
10010011.00001010.00000000.00000000 N . N . H . H
10010011.00001010.00000000.00000000 N . N . sN H. H

شكل ١٩-٢ ب وفي هذا المثال تم تخصيص ٥ بتات (5 bits) لتصميم الشبكة الفرعية

Class A network address 28.0.0.0
00011100.00000000.00000000.00000000 N . N . H . H
00011100.00000000.00000000.00000000 N . sN . sN H . H

شكل ١٩-٢ جـ في هذا المثال تم تخصيص ١٢ بت (12 bits) لتصميم الشبكة الفرعية

وبالإضافة إلى الحاجة إلى القدرة على إدارة الموارد المختلفة للشبكة، تدعم عملية التشبيك بعض الأمان وذلك لأن الوصول إلى الشبكات الفرعية الأخرى متاح من خلال خدمات الموجِّه فقط. كما أن حماية الوصول ربما تأتى من استخدام قوائم الوصول **Access Lists**، والتى تستطيع بدورها السماح بالوصول إلى الشبكة الفرعية أو عدم الوصول إليها بناءً على عدد من المعايير، مما يعطى المزيد من الأمان والحماية. لقد اكتشف بعض مالكى الشبكات ذات الفئة **Class A** والفئة **Class B** أن التشبيك الفرعي يتسبب فى إيجاد مصدر دخل للمؤسسة من خلال رعاية أو بيع عناوين **IP** الغير مستخدمة للآخرين.

وتعتبر عملية التشبيك الفرعي **Subnetting** إحدى الوظائف الداخلية للشبكة. فمن الخارج، يُنظر إلى الشبكة **LAN** كشبكة واحدة لا تحتوى على أية تفاصيل داخلية، وهذا يجعل جداول التوجيه صغيرة وعالية الكفاءة. فعلى سبيل المثال، فى حالة العنوان المحلى **147.10.43.14** بشبكة فرعية **147.10.43.0**، يرى العالم الخارجى الشبكة من الخارج بالرقم الرئيسى فى هذه الشبكة وهو **147.10.0.0**، والسبب فى ذلك أن عنوان التشبيك

المحلى 147.10.43.0 يكون متاحاً داخل شبكة LAN التى يتم تطبيق التشبيك الفرعى عليها.

إنشاء عنوان قناع الشبكة الفرعية Subnet mask address

يعتمد اختيار عدد البتس المستخدمة فى عملية التشبيك الفرعى على أكبر عدد أجهزة مضيفة مطلوبة لكل شبكة فرعية، ولذلك فإن فهم النظام الثنائي Binary System وقيمة كل بت بناء علي موقعها داخل البتات الثمانية أمراً ضرورياً عند حساب عدد الشبكات الفرعية والمضيفين والمنشئين كما يتضح من شكل ١٩-٣.

Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1

شكل ١٩-٣ تحديد قيمة كل بت بناء علي موقعه

ومن الممكن عدم تخصيص آخر ٢ بت إلى الشبكة الفرعية، لأن لهما دلالة معينة. فإذا تم استخدام جميع البتس، ما عدا آخر ٢ بت، فسنحصل على شبكات فرعية تحتوى على جهازين مضيفين فقط.

ويقوم قناع التشبيك بإمداد الموجِّه بالمعلومات اللازمة لتحديد مكان كل مضيف، داخل أى شبكة وأى شبكة فرعية، حيث يتم إنشاء قناع التشبيك باستخدام القيمة الثنائية 1 فى البتس الخاصة بالشبكة. ويتم تحديد البتس الخاصة بالشبكة الفرعية بإضافة القيمة المكانية للبتس التى تم اقتراضها. فعلى سبيل المثال، إذا تم اقتراض عدد ٣ بت، فإن القناع الخاص بالفئة الثالثة Class C يكون 255.255.255.224.

لتحديد عدد البتس المستخدمة، يحتاج مصمم الشبكة إلى حساب عدد الأجهزة المضيفة التى تحتاج إليها كل شبكة فرعية وكذلك عدد الشبكات الفرعية التى يحتاج إليها. فعلى سبيل المثال، إذا احتاجت الشبكة إلى ٦ شبكات فرعية، تحتوى كل منها على ٢٥ مضيف، يستطيع مصمم الشبكة فى هذه الحالة استخدام مخطط التشبيك الفرعى والذى يوضح الحاجة إلى ٣ بت فى قناع التشبيك الفرعي لاحتواء ٦ شبكات فرعية وهذا ما يؤدى إلى إنشاء ٣٠ جهاز مضيف لكل شبكة فرعية من الشبكات الست. ويرجع الفرق بين الأجهزة المضيفة المستخدمة والأجهزة المضيفة الكلية إلى استخدام أول عنوان متاح

كمعرف ID وآخر عنوان متاح كرقم عام لكل شبكة فرعية. ويعتبر اقتراض الرقم المناسب من البتس لاحتواء الشبكات الفرعية المطلوبة والأجهزة المضيفة الخاصة بكل شبكة عمل متزن وربما ينتج عنه عناوين أجهزة مضيفة غير مطلوبة فى أكثر من شبكة فرعية. ولا يمكن مع التوجيه الطبقى Classful routing استخدام هذه العناوين، وهذا على عكس التوجيه غير الطبقى Classless routing الذى يمكنه استعادة العديد من هذه العناوين.

ونستطيع استخدام الطريقة المستخدمة فى إنشاء مخطط التشبيك الفرعى فى حل جميع مشاكل التشبيك الفرعى، حيث تستخدم هذه الطريقة الصيغة التالية:

عدد الشبكات الفرعية القابلة للاستخدام = القيمة ٢ مرفوعة لعدد البتس المخصصة بالشبكة الفرعية أو البتس المقترضة مطروحاً منها القيمة ٢.

هكذا:

usable subnets = $2^{\text{power of borrowed bits}} - 2$

والسبب في طرح القيمة 2 أنها محجوزة لمعرف الشبكة Network ID .

ففى المثال السابق، لأننا نرغب فى الحصول على ٦ شبكات فرعية، يكون عدد البتس المطلوبة هى ٣ هكذا:

$6 = 2^{3} - 2$

أما الصيغة الخاصة بحساب عدد الأجهزة المضيفة القابلة للاستخدام فهى كما يلى:

عدد الأجهزة المضيفة القابلة للاستخدام = القيمة ٢ مرفوعة لعدد البتس المتبقية مطروحاً منها القيمة ٢.

هكذا:

usable Hosts = $2^{\text{power of remaining bits}} - 2$

ففى المثال السابق، لأن عدد البتس المتبقية هى ٥، فإننا نحصل على ٣٠ مضيف بكل شبكة فرعية هكذا:

$30 = 2^{5} - 2$

تطبيق قناع الشبكة الفرعية Subnet mask

نلاحظ أن عملية تفريع الشبكات تستخدم بعض بتات المضيف للحصول علي الشبكة الفرعية الجديدة. هذا يعني أنه في أي عملية تجزئة أو تفريع لشبكة فإن عدد الأجهزة في أي من الشبكات الفرعية يكون أقل من عدد أجهزة الشبكة الأصلية. تتمثل عملية التفريع في اقتراض عدد من بتات عنوان مضيف الشبكة الأصلية . فكلما كبر عدد البتات المقترضة من المضيف، زاد عدد الشبكات الفرعية وفي نفس الوقت نقص عدد الأجهزة في كل شبكة فرعية.

عدد الآحاد الإضافية في جزء قناع التفرع (عدد البتات المقترضة) هو الذي يولد أجزاء الشبكات الفرعية وعناوينها. أما الأصفار الباقية في القناع فتمثل عدد الأجهزة الممكن تشبيكها في كل شبكة فرعية. طبعاً هناك حالات استثنائية للقيم غير المستخدمة في عناوين الشبكة الفرعية وعناوين المضيفات والتي تتمثل في نفس القواعد التي تنطبق علي الشبكات العادية. هذا معناه عدم استخدام قيم كل البتات كأصفار أو آحاد لعناوين الشبكة الفرعية وعناوين المضيف.

لنري الآن مثالاً مفصلاً لعنوان شبكة من فئة C بقيمة 194.53.69.0 والذي نريد تقسيمه إلي شبكات فرعية. إذا استخدمنا 3 بتات من الثمانية الرابعة (آخر ثمانية بتات) لعنوان الشبكة الفرعية فالخمس بتات المتبقية تكون مخصصة لعنوان المضيف. وتكون قيمة قناع التفرع الخاصة بهذه الحالة كما يلي:

11111111.11111111.11111111.11100000

وهو ما يكافئ عشرياً القيمة التالية 255.255.255.224 لأن 224 هو المكافئ العشري للقيمة الثنائية 11100000. وهكذا يكون لدينا عنوان الشبكة الفرعية بطول 3 بت وعنوان المضيف بطول 5 بت.

من خلال هذا نستطيع أن نستخلص أن عدد الشبكات الفرعية التي نستطيع أن نحصل عليها من خلال 3 بت هي 2^3-2 أي 6 وتتمثل هذه القيم في 111,110,101,100,011,010.001.000

نعلم أنه من غير الممكن أن تكون قيمة أي عنوان (مميز) شبكة كلها أصفار أو كلها آحاد

فلذلك يمكن أن يأخذ مميز الشبكة الفرعية ذو 3 بتات أي واحدة من القيم الآتية:
110,101,100,011,010.001
أما بالنسبة للخمس بتات المخصصة للمضيف، فنستطيع من خلالها أن نحصل علي عدد 2^5-2 أي 30 من الاحتمالات والتي تتمثل في القيم التالية :
11111,11110 , ...,00011,00010,00001,00000
ولما كان من غير الممكن لأي مميز مضيف أن يحتوي علي أصفار (00000) أو آحاد (11111) فلذلك يتبقي لنا 30 قيمة تستطيع الأجهزة أن تتميز بها في أي شبكة فرعية والتي هي القيم العشرية التي تتراوح بين 1 (00001) إلي 30 (11110).
وهذا يعني عملياً أن استخدامنا لقناع تفرع ذي قيمة 255.255.255.224 يؤدي إلي إنشاء ستة شبكات فرعية تحتوي كل واحدة منها علي 30 مضيفا.
مهمتنا الآن هي إيجاد عناوين الشبكات الفرعية والتي يمكن الحصول عليها عند تفريع الشبكة 194.53.69.0 بواسطة قناع تفرع قيمته 255.255.255.224 .
طبعاً : أخذنا يعبن الاعتبار القيم غير الممكن استخدامها كعناوين (كمميزات) للشبكة أو المضيف.
فيما يلي عناوين الشبكات الفرعية التي تحصل عليها بعد ما اخترنا عنوان (مميز) المضيف كله أصفار . علماً أننا تعاملنا ثنائياً مع آخر ثمانية بتات وهذا لغرض التبسيط:

- عنوان الشبكة الأولي : استخدام 00100000 يؤدي إلي 194.53.69.32 .
- عنوان الشبكة الثانية : استخدام 01000000 يؤدي إلي 194.53.69.64 .
- عنوان الشبكة الثالثة : استخدام 01100000 يؤدي إلي 194.53.69.96 .
- عنوان الشبكة الرابعة : استخدام 10000000 يؤدي إلي 194.53.69.128 .
- عنوان الشبكة الخامسة : استخدام 10100000 يؤدي إلي 194.53.69.160 .
- عنوان الشبكة السادسة : استخدام 11000000 يؤدي إلي 194.53.69.192

لنري الآن عناوين الأجهزة في كل من الشبكات الفرعية وهذا بعد استخدامنا للقيم الممكن تقبلها في كل شبكة. الخمس بتات الخاصة بعنوان (بمميز) المضيف والتي تتراوح ثنائياً بين 11110 و 00001 تكون عناوين الأجهزة في الشبكات الفرعية الستة كما يلي :

في الشبكة الأولي من

194.53.69.33 إلي 194.53.69.62

في الشبكة الثانية من

194.53.69.65 إلي 194.53.69.94

في الشبكة الثالثة من

194.53.69.97 إلي 194.53.69.126

في الشبكة الرابعة من

194.53.69.129 إلي 194.53.69.158

في الشبكة الخامسة من

194.53.96.161 إلي 194.53.69.190

في الشبكة السادسة من

194.53.69.193 إلي 194.53.69.222

إذا أردنا الحصول علي عناوين البث (Broadcast) في كل من الشبكات الفرعية فما علينا إلا أخذ عنوان (مميز) المضيف كله، آحاد يعني 11111. تكون عناوين البث (Broadcast Addresses) لكل من الشبكات الفرعية كالآتي :

عنوان بث الشبكة الأولي : 194.53.69.63

عنوان بث الشبكة الثانية : 194.53.69.95

عنوان بث الشبكة الثالثة : 194.53.69.127

عنوان بث الشبكة الرابعة : 194.53.69.159

عنوان بث الشبكة الخامسة : 194.53.69.191

عنوان بث الشبكة السادسة : 194.53.69.223

فمن خلال هذه النتائج نستطيع أن نستخلص عدة أشياء منها :

- عناوين الأجهزة التي تستطيع أن تتصل مع بعضها دون اللجوء إلي موجه، كالأجهزة التي تحمل العناوين التالية : 194.53.69.99 و 194.53.69.120

- العناوين غير الممكن استخدامها عندما نجزئ شبكة ذات عنوان **194.53.69.0** بواسطة قناع **255.255.255.224** كالعنوان **194.53.69.96** والذي يكون مخصصاً كعنوان شبكة فرعية والعنوان **194.53.69.159** الذي يكون بدوره محجوز كعنوان بث شبكة فرعية.

كل هذا يساعد في عملية إعطاء العناوين للأجهزة بصفة سليمة ودون الوقوع في خطأ.

استخدام الشبكات الفرعية Class A وClass B

تتشابه عملية التشبيك الفرعي Class A وClass B مع تلك المستخدمة مع Class C، ما عدا وجود المزيد من البتس. فيمكنك فى حالة Class A تخصيص ٢٢ بت لحقل الشبكة الفرعية، بينما يمكنك تخصيص ١٤ بت فى حالة Class B.

ويعمل تخصيص ١٢ بت داخل عنوان Class B لحقل الشبكة الفرعية على إنشاء قناع شبكة فرعية **255.255.255.240** ويتم تخصيص البتس الثمانية بالجزء الثالث من العنوان بالقيمة **255** وهى القيمة الكلية للبتس الثمانية. كما يتم تخصيص ٤ بت بالجزء الرابع من العنوان بالقيمة **240**. (انظر شكل ١٩–٤)

Class B network address 147.10.0.0 (14 bits available)
10010011.00001010.00000000.00000000 N . N . H . H
10010011.00001010.00000000.00000000 N . N . sN . sN H

شكل ١٩–٤ في هذا المثال تم تخصيص ١٢ بت لتصميم الشبكة الفرعية.

كما يعمل تخصيص ٢٠ بت داخل عنوان Class A لحقل الشبكة الفرعية على إنشاء قناع شبكة فرعية **255.255.255.240**. ويتم تخصيص البتس الثمانية بالجزء الثانى والثالث من العنوان إلى حقل الشبكة الفرعية بالإضافة إلى ٤ بت من الجزء الرابع من العنوان. (انظر شكل ١٩–٥)

Class A network address 28.0.0.0 (22 bits available)
00011100.00000000.00000000.00000000 N . N . H . H
00011100.00000000.00000000.00000000 N . sN . sN . sN H

شكل ١٩–٥ في هذا المثال تم تخصيص ٢٠ بت لتصميم الشبكة الفرعية.

وفى هذه الحالة، يظهر جلياً التطابق التام بين قناع الشبكة الفرعية الخاص بعناوين Class A وعناوين Class B.

وإذا لم يكن القناع مرتبطاً بأحد عناوين الشبكة، فمن غير الممكن اكتشاف عدد البتس التى تم تخصيصها إلى حقل الشبكة الفرعية Subnet field.

فبغض النظر أيٍ من عناوين التصنيفين يحتاج إلى تشبيك فرعى، يتم استخدام أيٍ من الصيغ التالية:

Total subnets = $2^{\text{power of the bits borrowed}}$

Total Hosts = $2^{\text{power of remaining bits}}$

Usable subnets = $2^{\text{power of the bits borrowed}} - 2$

Usable hosts = $2^{\text{power of bits remaining}} - 2$

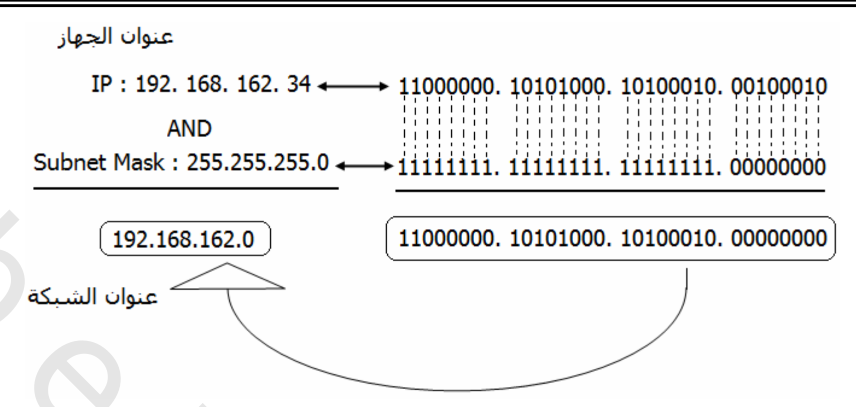
لكي تتمكن الأجهزة أن تتصل مع بعضها في نفس الشبكة الفرعية أو دون المرور عبر موجه (Router) فإنه من الضروري أن يكون لهذه الأجهزة نفس عنوان الشبكة ونفس عنوان الشبكة الفرعية. تؤدي عملية استخدام هذه الأقنعة إلي تجزئة أي عنوان شبكة من فئة A إلي عناوين من فئة B إلي C. كذلك الأمر إذا أردنا تجزئة عنوان من فئة B إلي عناوين من فئة C.

يبين الجدول التالي قيم أقنعة التفرع الممكن استخدامها في حالة تجزئة شبكة من فئة A إلي شبكات فرعية من فئة B أو تجزئة شبكة من نوع B إلي شبكات فرعية من نوع C وكذلك في حالة تجزئة شبكة من نوع C إلي شبكات فرعية.

فئة C Class C	فئة B Class B	فئة A Class A	عشري (Decimal)	ثنائي (Binary)
255.255.255.0	255.255.0.0	255.0.0.0	0	00000000
255.255.255.128	255.255.128.0	255.128.0.0	128	10000000
255.255.255.192	255.255.192.0	255.192.0.0	192	11000000
255.255.255.224	255.255.224.0	255.224.0.0	224	11100000
255.255.255.240	255.255.240.0	255.240.0.0	240	11110000
255.255.255.248	255.255.248.0	255.248.0.0	248	11111000
255.255.255.252	255.255.252.0	255.252.0.0	252	11111100
255.255.255.254	255.255.254.0	255.254.0.0	254	11111110
255.255.255.255	255.255.255.0	255.255.0.0	255	11111111

حساب عنوان شبكة فرعية باستخدام ANDing

كل ما ذكرناه حول أهمية استخدام أقنعة التفرع يتم ترجمته بواسطة بروتوكول طبقة الشبكة لمعرفة ما إذا كان جهاز الوجهة موجود علي نفس الشبكة المحلية الموجود عليها جهاز المصدر أم علي شبكة أخري. لمعرفة ذلك يؤدي جهاز المصدر عملية تسمي Logical ANDing وهي عملية تعني ضرب بت لبت Bitwise ANDing (يعني البت الأول مع الأول ، الثاني مع الثاني .....والبت 32 مع البت 32) لعنوانه IP مع قيمة قناع التفرع مما يؤدي إلي نتيجة تدل علي عنوان الشبكة الموجود عليها جهاز المصدر . بعدها يؤدي الجهاز نفس العملية والتي تخص جهاز الوجهة والتي من خلالها يحصل علي عنوان شبكة جهاز الوجهة. إذا كان العنوانان متطابقين يستنتج بروتوكول جهاز المصدر أن جهاز الوجهة موجود علي شبكته المحلية مما يمكنه من الاتصال به مباشرة. وفي حالة اختلاف عنواني الشبكتين فستنتج البروتوكول أن جهاز الوجهة موجود علي شبكة أخري، وللاتصال به لابد المرور عبر موجه. يبين الشكل التالي كيف تؤدي عملية Bitwise ANDing لعنوان IP أي جهاز مع قناع التفرع إلي معرفة عنوان الشبكة الموجود عليها الجهاز . (انظر شكل ١٩-٦)



شكل ١٩-٦ كيفية التعرف علي عنوان الشبكة باستخدام عملية ANDing

ملخص الفصل

شرحنا في هذا الفصل الحاجة إلي التشبيك الفرعي. ثم شرحنا كيفية عمل التشبيك الفرعي وأهميته. وأوضحنا وقدمنا مثالاً عملياً لكيفية تقسيم عنوان شبكة إلي شبكات فرعية بكل منها عدد من المضيفين. وأخيراً شرحنا كيفية حساب عنوان شبكة فرعية باستخدام **ANDing** .

تدريبات

١. ما هي العناوين التي تستخدمها حتي لا يري جهازك الآخرون علي الانترنت

٢. ماذا يمكن أن تتعلم من عنوان **IP** **172.16.10.22** (اختر إجابتين)

أ. **Class B**

ب. **Class C**

ج. عنوان المضيف **0.0.10.22**

د. عنوان الشبكة **172.16.10.0**

ه. عنوان الشبكة **172.0.0.0**

٣. أجر عملية **Bitwise ANDing** لكل زوج من العناوين التالية :

أ – **175.12.24.216 & 255.255.252.0**.

ب – **255.255.255.240 & 194.17.197.219**.

٤. من بين الأقنعة التالية ما هو القناع الذي يجزئ الشبكة إلي **62** شبكة فرعية؟

أ – 255.255.240.0

ب – 255.192.0.0

جـ – 255.255.255.252

د – 255.255.248.0

٥. علي أي جهاز يدل العنوان 127.0.0.1؟

أ – بوابة افتراضية.

ب – خادم DNS

جـ – الجهاز المحلي

د – خادم DHCP

٦. لدينا شبكة من الفئة C بعنوان 195.212.31.0 وقيمة قناع التفرع Subnet Mask = 255.255.255.252 ، أوجد ما يلي :

أ – عدد الشبكات الفرعية الممكن استخدامها .

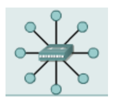
ب – عدد الأجهزة الممكن توصيلها في كل شبكة فرعية.

جـ – عناوين الشبكة الفرعية.

د– عناوين الأجهزة في كل شبكة فرعية.

هـ – عناوين البث في كل شبكة فرعية .

٧. هل تستطيع الأجهزة ذات العناوين : 195.212.31.5 و 195.212.31.9 أن تتصل ببعضها مباشرة دون العبور علي موجه ؟



الباب السابع
إدارة الشبكة

الفصل العشرون : مهام إدارة الشبكة

الفصل الحادي والعشرون : عوامل مساعدة في إدارة الشبكة

الفصل الثاني والعشرون : استكشاف مشكلات الشبكة وإصلاحها



بعد إعداد الشبكة وتشغيلها يلزم المحافظة على استمرارها فى العمل بشكل جيد. هذا بالضبط ما نعنيه بإدارة الشبكة ، بانتهاء هذا الفصل سنتعرف على

- *مدير الشبكة*
- *تسجيل معلومات الشبكة*
- *إدارة الشبكة*
- *إدارة شئون مستخدمي الشبكة*
- *أدوات مدير الشبكة*

مدير الشبكة Network Administrator

مدير الشبكة هو الشخص المسئول عن سلامة الشبكة ، ويجب أن يكون مدير الشبكة على قدر كبير بالمعلومات التي تؤهله لإدارة الشبكة والحفاظ عليها فى حالة جيدة مثل المكونات المادية للكمبيوتر و أجهزة الشبكة وبروتوكولات الشبكة ، ونظم تشغيل الشبكات. لقد عرضنا في الفصول المتقدمة قدراً كبيراً من المعلومات التي يجب أن يكون مدير الشبكة علي دراية تامة بها مثل المكونات المادية للكمبيوتر وبروتوكولات الشبكة ونظم تشغيل الشبكات وكيفية ربط الشبكات وتجميعها. تساعد الخبرة الجيدة والحس العام مدير الشبكة في الحفاظ علي الشبكة بحالة جيدة.

تختلف المهام المنوطة بمدير الشبكة تبعا لحجم المؤسسة التي يعمل بها و حجم الشبكة وطريقة عملها . فى الشركات الصغيرة قد يقوم موظف متخصص فى دعم الشبكات بمعالجة المشكلات اليومية وتوفير الدعم وعندما تحتاج لمهام صعبة أو متقدمة مثل عمليات تخطيط بناء الشبكة أو تركيبها ، تلجأ إلى مهندس متخصص أو مستشار فى أمور الشبكات. فى الشركات الصغيرة هذه يكون متخصص دعم الشبكات هو مدير الشبكة. فى الشركات الكبيرة تناط مسئوليات أكبر بمدير الشبكة حيث يعمل معه مهندسي شبكات ومتخصصى دعم شبكات ويتولى هو الإشراف على الجميع

قد تلجأ بعض الشركات الصغيرة إلى شخص محترف فى نظم الكمبيوتر والشبكات ليعمل لديها بعض الوقت ويقوم متخصص دعم الشبكات بباقي العمل كل الوقت .

وفيما يلى نعرض لبعض المواصفات التي يجب أن تتسم بها وظيفة مدير الشبكة

- يجب أن يخصص وقتا كافيا لإدارة الشبكة خصوصا فى الشبكات الكبيرة حتى تتاح له الفرصة للتعرف على تفاصيل الشبكة .
- يجب أن تكون لديه صلاحيات اتخاذ القرارات التي تتعلق بالشبكة مثل تحديد صلاحيات كل مستخدم . ونوع الملفات التي ستوضع على الجهاز الخادم . ومواعيد وكيفية إجراء النسخ الاحتياطي للملفات ....الخ
- يجب أن يتسم مدير الشبكة بالنظام واليقظة وأن يكون دقيقا فى عمله فيتأكد من عدم

تجاوز أى مستخدم للصلاحيات المخولة له ومن تطبيق الإجراءات السليمة لمقاومة الفيروسات على كل جهاز ومن إجراء النسخ الاحتياطي في مواعيده .

- يجب أن يكون على دراية تامة بالشبكة التي يديرها ، خصوصا إذا لم يكن هو الشخص الذي قام بتركيبها . ويتضح ذلك من البند التالي .

تسجيل معلومات الشبكة

فى النقطة الأخيرة لسمات وظيفة مدير الشبكة قلنا أنه يجب أن يكون على دراية تامة بالشبكة التي يديرها . و لذلك فان من الواجبات الرئيسية لمدير الشبكة تسجيل أحدث المعلومات عنها ، والاحتفاظ بها فى ملف مخصوص .

يمكن أن يشمل هذا الملف على معلومات وافية عن :

- مخطط تفصيلي للشبكة يشتمل على مواقع الأجهزة الموجودة فى الشبكة . مع توضيح التغيير الذى طرأ عليها وتاريخه وأسبابه .
- وصف تفصيلي لكل جهاز من أجهزة الكمبيوتر وللجهاز الذى يعمل كجهاز خادم .يمكن أن يتضمن الوصف التفصيلي للجهاز معلومات عن مكانة ومن يستخدمه والمكونات التي يشتمل عليها (مثلا نوع وسرعة المعالج ، وحجم الذاكرة ، وحجم القرص الصلب ونوع بطاقة الفيديو، والبرامج المحملة عليها ،.........الخ
- قائمة تفصيلية لموارد الشبكة والحروف المخصصة لمحركات الأقراص على الجهاز الخادم .
- نظام النسخ الاحتياطي .

إدارة الشبكة

عندما ترى مشروعا كبيرا ، يجب عليك الاستفادة من برامج إدارة المشروعات المتاحة فى الأسواق ومنها على سبيل المثال برنامج **Microsoft Project** وبرنامج **Primavera** تسهل برامج إدارة المشروعات تعقب المهام والموارد والموظفين كذلك توفر معظم برامج إدارة المشروعات طرق عرض مختلفة لبيانات المشروع . من الفوائد التى تحصل عليها من

استخدام برامج إدارة المشروعات مثل برنامج **Microsoft Project** أنك يمكنك توصيف كل مهمة في المشروع . حيث تكون مستقلة عن المهام التي يجب استكمالها قبل أن تبدأ مهمة معينة .

يجعلك هذا النوع من تعقب المشروعات آمناً . حيث أنك تتعامل مع كل مهمة بالترتيب المناسب مع الانتقال من بداية المشروع نحو مرحلة الاكتمال . كذلك تسهل برامج إدارة المشروعات إنشاء تقارير مرتبطة بأي مشروع .

بعد هذه المقدمة عن برامج إدارة المشروعات وفائدتها عموما والتي بالقطع تفيدك فى إدارة الشبكة، نتحدث بشيء من التفصيل عن مهام مدير الشبكة ، حيث يشترك جميع مديرى الشبكات فى الأمور التالية :

- متابعة حالة الأجهزة والكابلات وكروت الشبكة وأجهزة التوصيل (**Hub**) أو أجهزة التبديل (**Switch**) وغيرها من الأجهزة ، بالإضافة إلى نظام التشغيل .
- العمل على تطوير الشبكة باستمرار بأحدث الأجهزة والمشاركة فى كل قرار يتعلق بشراء أجهزة جديدة واقتراح شراء أفضل الأجهزة لشبكته مثل شراء أجهزة كمبيوتر تحتوى على بطاقة شبكة مثبتة عليها .
- عند إضافة جهاز جديد للشبكة ، يقوم مدير الشبكة بمجموعة مهام لتعمل ضمن الشبكة الموجودة . من هذه المهام تخصيص اسم (**ID**) وكلمة مرور للمستخدم الجديد . وتحديد الصلاحيات التي تخول إليه في التعامل مع الملفات وباقي الأجهزة .
- متابعة الجديد في نظم التشغيل وما تصدره الشركات المنتجة مثل **Microsoft** و **Novell** ، حيث جرت العادة أن تصدر الشركات في الفترة الأخيرة مابين ظهور إصدار وآخر برامج إصلاح ومجموعات خدمات لإصلاح المشكلات التي تواجه عملائها .
- إجراء النسخ الاحتياطي بصورة منتظمة ، لأن المدير هو المسئول في حالة ضياع البيانات بسبب عدم وجود نسخ احتياطية في الشركة.
- تثبيت برامج الكشف علي الفيروسات وتثبيت جدار النار لتأمين الشبكة من

الفيروسات والقرصنة.

- متابعة الملفات التي يخزنها المستخدمون علي وحدة الخدمة وحذفها حال عدم الحاجة إليها لتوفير المساحة التي تشغلها.

إدارة شئون مستخدمي الشبكة

لا تقتصر مهام مدير الشبكة علي إدارة الجوانب الفنية في الشبكة . إنما عليه أن يكون علي دراية بإدارة شئون مستخدمي الشبكة للارتقاء بمستوياتهم وبما يمكنهم من أداء عملهم بسهولة ويسر . ومن الأمثلة علي ذلك أن يحرص علي تقديم قدر كاف من المعلومات عن الشبكة وكيفية التعامل معها لجميع المستخدمين . لأنه مالم تتوفر لدي المستخدمين هذه المعلومات فقد يتسببون في مشكلات عديدة بدون تعمد .

يجب أن يقدم مدير الشبكة للمستخدمين دورة تدريبية تشرح لهم بنية الشبكة ومكوناتها والمعلومات التي تلزمهم أثناء تعاملهم معها. والأهم من كل ذلك أن يتحلي مدير الشبكة بالمرونة الكافية عندما يتلقي شكوي من أحد المستخدمين. وأن يسارع في حلها حتي لايقع المستخدم في خطأ إذا حاول حلها بنفسه.

أدوات مدير الشبكة

بالطبع يحتاج مدير الشبكة إلي أدوات مثل المفك والمطرقة ومكبس الكابلات ، ولكني هنا لا أقصد هذه الأدوات. الأدوات التي أقصدها هنا هي مجموعة برامج هي بمثابة أدوات لمدير الشبكة لا يستغني عنها للمحافظة علي استمرار عمل الشبكة بشكل جيد .

برامج الإصلاح

برنامج الإصلاح عبارة عن برنامج تحديث صغير يعمل علي إصلاح الأخطاء الصغيرة التي تظهر من وقت لآخر، تعمل أغلب هذه البرامج علي إصلاح الأخطاء الأمنية التي يكتشفها المتسللون إلي الشبكات . لجميع إصدارات **Windows** يمكن الحصول علي برامج الإصلاح من موقع **Windows Update Web**. يمكن الوصول إليه من الموقع **Windows Update.Microsoft.Com** .

يعمل .Windows Update علي إنشاء قائمة برامج الإصلاح وغيرها من المكونات التي تستطيع تنزيلها وتثبيتها. يمكن إعداد **Windows Update** بحيث يعلمك تلقائيا بالتحديثات بمجرد ظهورها بدلا من أن تتولي البحث بنفسك عن برامج الإصلاح.

البرامج الإدارية

يحصل مدير الشبكة علي أغلب البرامج الإدارية التي يحتاج إليها في إدارة الشبكة من برنامج الشبكة نفسه. يجب أن يقرأ مدير الشبكة الكتيبات الإرشادية التي تأتي مصاحبة لبرنامج الشبكة جيدا ليعرف الأدوات المتاحة لإدارتها .

برنامج **Microsoft System Information**

يشكل هذا البرنامج وهو موجود في نظام **Windows** أهمية كبيرة كمصدر معلومات عن الشبكة .

برنامج **Norton Utilities**

هذا البرنامج يتضمن إمكانيات هائلة لإصلاح محركات الأقراص وإعادة تنظيم بنية دليل القرص الصلب ، والحصول علي معلومات عن الجهاز الذي تستخدمه ومكوناته. برنامج **Norton Utilities** من إنتاج شركة **Symantec**.

أداة **Hotfix Checker**

توفر شركة **Microsoft** أداة اسمها **Hotfix Checker**. تعمل هذه الأداة علي مسح أجهزة الكمبيوتر لتحديد برامج الإصلاح المراد استخدامها . قم بتنزيل هذه الأداة من موقع **Microsoft** علي الويب . اذهب الي الموقع **WWW.MICROSOFT.COM** ثم ابحث عن **HFNETCHK.EXE**

الوظائف المرتبطة بإدارة الشركة

توجد بعض الوظائف المهنية المرتبطة بصورة مباشرة أو غير مباشرة بإدارة الشبكة. وسنبدأ من أسفل إلي أعلي في تدرج الوظائف.

- *الدعم الفني* : يساعد موظفوا الدعم الفني المستخدمين علي تشخيص المشكلات

التي تصادفهم أثناء تعاملهم مع الكمبيوتر أو الشبكات، كعجزهم عن تسجيل الدخول إلي الشبكة أو فقد ملف ما. وعادة يقدمون لهم الحلول المناسبة عبر الهاتف أو عبر الشبكة، ويجب أن يلم موظف الدعم الفني بنظام شركته وطبيعة المستخدم والمشكلات المحتمل أن تواجهه.

- ***متخصص دعم شبكة LAN*** : يكون مسئولاً عن إعداد الأجهزة الجديدة وتوصيلها بالشبكة والتأكد من تثبيت البرامج المناسبة. يكون مستوي موظفي دعم شبكة LAN أعلي من مستوي موظفي الدعم الفني، ويمكن أن يكون موظف دعم الشبكة مسئولاً عن بعض الأعمال مثل إعمال النسخ الاحتياطي للشبكة أو صيانة وحدة الخدمة.
- ***مدير الشبكة*** : أوضحنا الكثير من وظائف ومهام مدير الشبكة بالإضافة إلي ذلك فإن مدير الشبكة مسئول عن تخطيط البنية الأساسية للشبكة وتنفيذها وصيانتها. يجب أن يلم تماماً بنظم التشغيل الشبكات وأجهزة الشبكات.
- ***مدير تكنولوجيا المعلومات (IT Director)*** : هو الشخص المسئول عن التخطيط والتنفيذ الفعلي للبنية الأساسية للشبكة، وهو إما أن يمثل الإدارة العليا أو يكون مسئولاً أمام الإدارة العليا ولذلك فهو يعد التقارير ويكون مسئولاً عن الميزانيات والمخزون ..... الخ .

ملخص الفصل

ناقشنا في هذا الفصل بعض الصفات التي يجب أن يتسم بها مدير الشبكة ثم نافشنا مهام مدير الشبكة والواجبات المنوطة به.

ناقشنا أيضا الأدوات والبرامج التي تساعد مدير الشبكة في الحفاظ علي الشبكة تعمل علي أكمل وجه وخصوصاً في المؤسسات الكبرى. وأخيرا ألقينا نظرة علي الوظائف المرتبطة بإدارة الشبكة .

تدريبات

١. أذكر ثلاثة من الصفات التي يجب أن يتسم بها مدير الشبكة الناجح؟

٢. ضع علامة (✓) أمام العبارة الصحيحة وعلامة (✖) أمام العبارة الخاطئة.

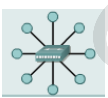
أ. لا يستغني مدير الشبكة عن مجموعة من البرامج تساعده في أداء عمله.

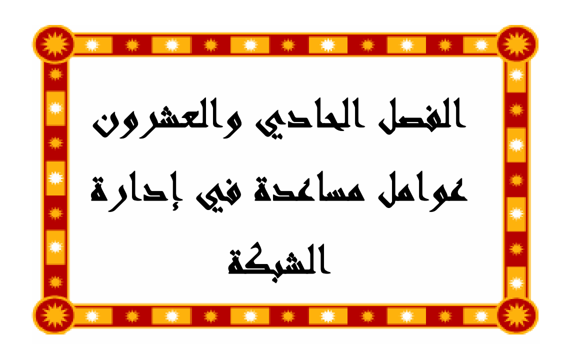
ب. في المنشآت الصغيرة ليس من الضروري تعيين مدير متخصص للشبكة

ج. يحتفظ مدير الشبكة بمعلومات الشبكة لنفسه ولا داعي لتسجيل معلوماتها في ملف.

د. إدارة شئون مستخدمي الشبكة تخص المدير المالي وليس مدير الشبكة شأن بها.

٣. أذكر ثلاثة من المهام الأساسية لمدير الشبكة ؟





الفصل الحادي والعشرون
عوامل مساعدة في إدارة الشبكة

يجب أن يكون لدي جميع المؤسسات حتي الصغيرة منها خطـــة للاحتفاظ ببياناتها ومواكبة تطورات تكنولوجيا الاتـــصالات. هذا ما سنتناوله في هذا الفصل. بالانتهاء مـــن هـــذا الفـــصل ستتعرف علي :

- *مواكبة تطورات تكنولوجيا الاتصالات*
- *ترقية الشبكة*
- *نسخ البيانات احتياطيا*
- *التخطيط للاسترداد من الكوارث*
- *إنشاء مكتبة*
- *استشارة الخبراء*

مواكبة تطورات تكنولوجيا الاتصالات

يجب أن يكون مدير الشبكة مطلعا علي أحدث التطورات في مجال الكمبيوتر. غالبا ما يلجأ معظم المستخدمين لحل مشاكلهم، وغالبا ما يتوقعون أن يكون مدير الشبكة علي علم بأحدث التقنيات والتطورات . وهذا يدعوهم للاستفسار عن أمور عديدة قد تبدو أحيانا محرجة ومعقدة .

ننصح مدير الشبكة بمجموعة من الأمور التي تجنبه الحرج عندما يتعرض لأسئلة المستخدمين وليبقي علي علم بأحدث التطورات والتقنيات في عالم الكمبيوتر .

- احرص علي شراء أو الاشتراك في واحدة علي الأقل من المجلات المتخصصة في الكمبيوتر وأخري من المتخصصة في الشبكات. وبهذا تكون علي علم بأي تطورات في عالم الكمبيوتر بصفة عامة وفي مجال الشبكات بصفة خاصة .
- من الأمور المفيدة أيضا الرسائل الإخبارية علي البريد الالكتروني. اشترك في الرسائل الإخبارية لتكون علي علم بالنظم التي تستخدمها في شبكتك .
- اختر من المجلات الموضوعات التي تناسب مستوي معرفتك بعد فترة يتحسن مستواك وتزيد معلوماتك وتستطيع أن تقرأ موضوعات فنية متقدمة تفيدك في عملك .

ترقية الشبكة

كل يوم نسمع عن جديد في عالم الكمبيوتر . سواء في الأجهزة أو البرامج . مع التغيير السريع في الأجهزة والبرامج ستضطر إلي اللجوء إلي ترقية شبكتك . طبعا من الأفضل أن تصمم شبكتك من الأول بحيث لا تضطر إلي ترقيتها إلا بعد مدة طويلة. لأن مهمة المدير الناجح أن يحافظ علي الشبكة في أفضل حالة ممكنة. قد تحتاج إلي استبدال الخادمات وأجهزة الوحدات التابعة ونظم تشغيل الشبكة، وتطبيقات الوحدات التابعة. وذلك حسب ما يتطلبه أسلوب الترقية الذي ستلجأ إليه .

يجب أن تأخذ في اعتبارك عند اتخاذ قرار الترقية التكلفة المادية المالية للشركة. إذ في كثير من الأحيان يمكنك الاستغناء عن عمليات الترقية غير الضرورية أو اللجوء إلي أساليب غير مكلفة .

إن من طبيعة الأمور أن تنمو شركتك وتتوسع بعد فترة من الزمن خصوصا إذا كانت الشركة ناجحة في عملها. وفي هذه الحالة سوف تحتاج إلي التخطيط لنمو الشبكة آخذا في اعتبارك الأمور التالية :

- توفير معلومات واقعية عن مكونات كل كمبيوتر . لأنك لا بد أن تعرف ماذا يوجد بداخل الكمبيوتر . حتي تحدد ما إذا كان من الممكن ترقيته أو استبداله بسهولة .
- معرفة ما إذا كان وضع أجهزة تقبل بترقية زائدة أم لا . بمعني معرفة هل إضافة معالج أسرع وذاكرة أكبر للجهاز لزيادة فعالياته ممكنة أم لابد من استبدال أجزاء أخري وأحيانا حتي الأجهزة كلها ..
- تحديد مواصفات قياسية للأجهزة . لأن هذا يساعدك عند اكتشاف الحاجة إلي ترقية جهاز ما في اتخاذ قرار لترقية باقي الأجهزة المشتركة في نفس المواصفات .

نسخ بيانات الشبكة احتياطيا Back Up

تحتاج إلي عمل خطة دقيقة لنسخ بيانات الشبكة احتياطيا لأسباب عديدة منها علي سبيل المثال الكوارث الطبيعية التي قد تتعرض لها مثل الحريق أو الفيضانات أو الزلازل التي تتعرض لها المدن التي تقيم بها والتي توجد بها شبكتك. إن إنشاء خطة نسخ احتياطي وتنفيذ هذه الخطة، يعد جانباً مهما إدارة الشبكة قد تري أن الشبكة تعمل بصورة سلسة ومنتظمة ولا توجد مشكلات في سجلات وحدات الخدمة وجداول مراقبة الأداء. عندها قد لا تصدق أن عطلاً مفاجئاً قد يحدث وينتج عنه فقد البيانات. ولكن إذا وقع المحظور وحدث ذلك فستجد نفسك في ورطة شديدة. لذلك من الأفضل افتراض أن انهياراً في الشبكة سوف يحدث في يوم ما وعليك الاستعداد بصورة كافية لهذا اليوم.

إستراتيجية النسخ الاحتياطي

مشكلات الشبكة في غالب الأحيان لا تكون ناتجة عن عوامل طبيعية . فقد تتعرض الأجهزة للعبث أو التحطيم من قبل شخص مخرب. من الضروري ان تضع خطة لمواجهة المشكلات التي تظهر في الشبكة آخذا في الاعتبار مايلي :

- ✓ وضع برنامج منتظم لنسخ البيانات (سنشرح فيما يلي من هذا الفصل كيفية وضع هذا البرنامج وتنفيذه) .
- ✓ احرص علي الاحتفاظ بأقراص أو أشرطة النسخ الاحتياطية في مكان آمن بعيدا عن أجهزة الكمبيوتر. يمكنك أيضا حفظ مجموعة من هذه الأقراص أو الأشرطة في مكان أخر بعيدا عن موقع الأجهزة والشركة .
- ✓ احرص بشدة علي قائمة الجرد التي تحتوي معلومات تفصيلية عن مكونات أجهزة الشبكة .فهي مهمة جدا لك ويفضل أن تحتفظ بأكثر من نسخة منها .
- ✓ احرص علي توفير أكبر قدر ممكن من المعلومات عن أجهزة الكمبيوتر والشبكات لأكثر من شخص. حيث أن قصر العلم بكافة الجوانب الفنية للأجهزة والشبكة علي مسئول الصيانة فقط يحدث ارتباكا شديدا في العمل عندما يتغيب هذا الشخص .

ويجب عند التخطيط لوضع إستراتيجية فعالة للنسخ الاحتياطي التفكير في الأمور الآتية:

- ماهي البيانات التي يجب عليك نسخها احتياطيا .
- ماهو عدد المرات التي يجب أن تقوم فيها بعمل النسخ الاحتياطي
- نوع الوسائط التي ترغب في إجراء النسخ الاحتياطي عليها. (أشرطة أو أقراص مغناطيسية) ، أم محركات أقراص نقالة مثل **Zip** و **Jaz** أو أقراص **CD-Rom** أو **DVD**
- تحديد هل ستشمل عملية النسخ الاحتياطي كل المجلدات والملفات والبيانات الموجودة علي الشبكة أم ستشمل ملفات معينة ومتي يتم عمل نسخ احتياطي لجميع الملفات ، ومتي يتم عمل نسخ احتياطي لملفات معينة.

أنواع النسخ الاحتياطي

توجد ثلاث طرق لإجراء النسخ الاحتياطي : الأولي **Full Backup** (النسخ الاحتياطي التام) ، والثانية **Differential Backup** (النسخ الاحتياطي المتباين) والثالثة **Incremental Backup** (النسخ الاحتياطي التزايدي) .

النسخ الاحتياطي التام أو الكلي Full Backup

هو النسخ الاحتياطي العادي أو اليومي، ويتم عادة كل أسبوع أو كل شهر حسب حجم العمل، ويأخذ كل الملفات التي تحددها للنسخ الاحتياطي وينسخها احتياطياً (بغض النظر عن كيفية تعليم الملفات) بعد الانتهاء من عملية النسخ الاحتياطي ، يتم تغيير سمات الملفات التي نسخت لتوضيح أنها تم نسخها احتياطياً. بمجرد أن يحدث تغيير للملفات أو تعديل بها بعد النسخ الاحتياطي سوف تتغير العلامة وتشير إلي أن الملف لم يتم نسخه احتياطياً منذ إجراء التغييرات الأخيرة، وسيتم نسخه احتياطياً في أول مرة يجري فيها نسخ احتياطي تام.

النسخ الاحتياطي المتباين ***Differential Backup***

ومعناه عمل **Backup** لكل الملفات التي أنشئت أو عدلت منذ آخر **Backup** قمت به دون أن يضع علامة علي أن هذه الملفات أخذ لها **Backup**. فمثلاً إذا أنشأت ملف يوم السبت وقمت في المساء بعمل **Differential Backup** فسيتم حفظ الملف (عمل **Backup** له) دون وضع إشارة تدل علي حفظه فإذا قمت في اليوم التالي (يوم الأحد) بعمل **Differential Backup** فإن هذا الملف سيتم حفظه سواء قمت بتعديله أم لم تقم. هذا الإجراء يتسبب في ربط عملية الـ **Backup** .

النسخ الاحتياطي التزايدي ***Incremental Backup***

ومعناها عمل **Backup** لكل الملفات التي أنشئت أو عُدلت منذ آخر **Backup** قمت به، ويضع علامة أمام الملفات التي يحفظها تدل علي أن هذه الملفات تم عمل **Backup** لها وباستخدام المثال السابق إذا أنشأت ملف يوم السبت وقمت بعمل **Incremental Backup** في مساء السبت فسيتم حفظ الملف **Backup** ووضع إشارة تدل علي حفظه. فإذا قمت في اليوم التالي (يوم الأحد) بعمل **Incremental Backup** فلن يتم عمل **Backup** له إلا إذا تعدل أو تغيير منذ عمل **Backup** يوم السبت. ولهذا فهو يأخذ وقتاً أقل في عملية الـ **Backup** لأن الملفات الجديدة أو

التي عدلت فقط هي التي تؤخذ في الحسبان .

تحديد الملفات المطلوب نسخها احتياطياً Selecting Files to Backup

عندما تنوي عمل نسخ احتياطي لملفات يجب أن تأخذ في اعتبارك أولويات الملفات كما يلي :

- الملفات الضرورية للنظام مثل ملفات نظام التشغيل وملفات التسجيل وملفات البرامج التطبيقية.
- ملفات البيانات الضرورية مثل المستندات التي تنشئها وتحفظها. فملفات البيانات التي تنشئها تأخذ عادة وقت قليلاً وتحتاج لعمل حفظ لها لفترات متقاربة ، أو يومية مثلاً أما ملفات النظام تأخذ وقتاً طويلاً ولا تتغير غالباً فيمكن عمل حفظ لها علي فترات متباعدة (شهرية مثلاً) .

عمل جدول للنسخ الاحتياطي Backup

إذا كانت أعمالك كبيرة وبياناتك كثيرة يفضل أن تضع نظاماً للنسخ الاحتياطي **Backup** عبارة عن جدول، يبين فيه مواعيد عمل **Backup** كامل ومواعيد عمل النسخ الاحتياطي **Backup** جزئي. النسخ الاحتياطي **Backup** الكلي عبارة عن صورة كاملة من القرص الصلب ويتم عادة كل أسبوع أو كل شهر حسب حجم عملك. أما النسخ الاحتياطي **Backup** الجزئي فيتم عادة يومياً أو أسبوعياً حسب حجم عملك أيضاَ، وفيه يتم نسخ الملفات التي تتغير فقط منذ آخر **Backup** إلي يوم عمله. ويجب تخصيص مجموعة أقراص أو شريط مغناطيسي مستقل لكل من هذين النوعين، فإذا تعطل القرص الصلب أو سرق يمكن استرجاع المجموعة (أو الشريط) التي تحتوي علي النسخ الاحتياطي **Backup** الكلي ، أما إذا تلفت الملفات الخيرة نتيجة الحذف أو انقطاع التيار الكهربي فيمكن إرجاع المجموعة (أو الشريط) التي تحتوي علي النسخ الاحتياطي **Backup** الجزئي ثم إعادة تشغيل أو كتابة البيانات التي فقدت بعد آخر تعديل.

برامج النسخ الاحتياطي

تحتوي جميع إصدارات Windows علي برامج نسخ احتياطي . كمـا أن اغلـب وحدات تشغيل الشرائط تحتوي علي برامج نسخ احتياطي أسرع وأكثر مرونة من النسخ الاحتياطي المعتاد علي نظام Windows. كما ان هناك برامج للنسخ الاحتياطي معـدة خصيصا للاستخدام في الشبكات الكبرى التي تحتوي علي أكثر من جهاز خادم .

لا تقتصر وظيفة برامج النسخ الاحتياطي علي نسخ البيانات من القرص الصلب لجهازك إلي شريط . أو قرص مغناطيسي أو أي وحدة ضغط أخري .

تستخدم برامج النسخ الاحتياطي تقنيات ضغط البيانات حتى تتمكن من حفظ أكبر قدر من البيانات على أقل وسائط تخزين . فإذا كان معدل ضغط البيانـات هـو ٢ : ١ فـان الشريط الذى تبلغ سعته ٢٠ جيجا بايت يستطيع أن يحمل بيانات مضغوطة قـدرها ٤٠ جيجا بايت. تسمح لك برامج النسخ الاحتياطي بتتبع البيانات التى تم نسخها ، وتلك التى لم يتم نسخها بعد . كما انها تتيح خيارات للنسخ الاحتيـاطى مثـل نـسخ Full آو Differential او Incremental كما سبق توضيحه فى البند السابق .

نسخ البيانات على الجهاز الخادم / التابع .

عند نسخ بيانات الشبكة يمكن تشغيل برنامج النسخ الاحتيـاطي بطـريقتين . الأولى تشغيله على الجهاز الخادم نفسه والثانية تشغيله من احد الأجهزة التابعـة المتـصلة بالشبكة .

فى حالة تشغيل البرنامج على وحدة الجهاز الخادم يتأثر الجهاز الخادم بذلك و يحدث بطء فى اتصال المستخدمين بهذا الجهاز . أما إذا تم تشغيل الجهاز من جهاز تابع فـسيتدفق كـم البيانات المراد نسخه عبر الشبكة مما يسبب انخفاض سرعة الشبكة بالكامل .

لذلك ننصح أن يتم النسخ بعد انتهاء العمل أو خلال الساعات التى يتوقف فيها العمل ولا يحاول أى مستخدم الوصول إلى الشبكة حفاظ على أدائها. وعموما تحتوى عملية نـسخ البيانات أثناء استخدام أشخاص متصلون بملفات على الجهاز الخادم على مخاطرة كـبيرة .

فإذا قمت بعملية النسخ أثناء استخدام البعض لملفات موجودة علـــى الجهـــاز الخـــادم ، فسيتجاوز برنامج النسخ الاحتياطي أى ملفات يعمل عليها المستخدمون . وغالبا تكـــون هذه الملفات أهم ما يجب نسخة لأنها تكون الأكثر استخداما وتعديلا.

فيما يلى بعض النصائح المتعلقة بالنسخ الاحتياطي على الجهاز الخادم أو الجهاز التابع :

- عادة يكون النسخ الاحتياطي على الجهاز الخادم بطيئا فى حالة إجرائه أثناء ســـاعات العمل المكثفة حيث يكثر عدد مستخدمى الشبكة ويري البعض أن نسخ البيانـــات مباشرة من الجهاز الخادم أفضل من نسخها من الجهاز التابع حتى لا تنتقل البيانـــات عبر الشبكة .
- لتحسين سرعة عملية النسخ على الشبكة ، استخدم جهاز **Switch** (سويتش) بدلا من جهاز **Hub** العادي لربط أجهزة الجهاز الخادم والجهاز التابع الذى تـــتم عليـــه عملية النسخ . وبهذا لن تؤثر البيانات المتدفقة بين الجهاز الخادم والجهاز التابع على بقية أجزاء الشبكة .
- يفضل أن يكون شخص واحد مسئول عن عملية النسخ ويجب تخصيص كلمة مرور وكود خاص به (**ID**) ومنحة حق الوصول إلى جميع الملفات على الجهـــاز الخـــادم .ويجب ألا يعرف أى شخص آخر الكود المخصص لهذا الشخص حتى لا يتمكن من الدخول إلى الشبكة ونسخ بيانات سرية أو غير مسموح بخروجها.
- يجب غلق جميع الملفات قبل إجراء النسخ الاحتياطي .لأن الملفات المفتوحة لن تشملها عملية النسخ الاحتياطي. للتأكد من ذلك يمكنك إلغـــاء تـــسجيل دخـــول جميـــع المستخدمين على الشبكة قبل بدء عمليات النسخ الاحتياطي

التخطيط للاسترداد في حالة الكوارث

إذا كان الهدف من استرتيجية النسخ الاحتياطي للشبكة هو في النهاية استرداد البيانات في حالة وقوع أي نوع من الكوارث سواء كانت كوارث داخلية تخص المؤسسة أو خارجية كالزلازل أو الحروب أو الفيضانات فيجب ألا تنتظر حتى تقع الكارثـــة حـــتى نفكـــر في

التخطيط للاسترداد من الكوارث. إنما الصح أن يقوم مدير الشبكة بوضع خطط تسمح له بوضع البيانات المهمة في أيدي من يحتاجون إليها. بعبارة أخرى يجب أن يضع خطة استرداد من الكوارث متعددة الأوجه وتتوقع مستويات مختلفة من الكوارث بحيث يناسب كل نوع من الكوارث خطة قد لا تناسب نوع آخر. فمثلاً في حالة وقوع حريق دمر شبكة وأجهزتها، فإن الخطة المناسبة للاسترداد من كارثة الحريق هي استخدام بيانات النسخ الاحتياطي لإعادة بناء خادمات بيانات الشبكة في موقع جديد وتوفير إمكان وصول شبكة إلي هذه البيانات . أما في حالة الفيضان الذي يعوق الموظفين من الوصول إلي مكاتبهم فإن من المناسب في هذه الحالة أن يضع مدير الشبكة خطة استرداد البيانات من الكوارث بحيث يكون الموظفون على اتصال ويعملون من منازلهم. وقد تملي عليه خطة الاسترداد تنشيط VPN أو الاتصال الهاتفي الذي يسمح للموظفين بالعمل من المنزل.

من هذه المقدمة نفهم أن لكل نوع من الكوارث خطة استرداد مختلفة

وضع خطة استرداد من الكوارث

تتطلب خطة الاسترداد من الكوارث عدد من العناصر:

- البنية الأساسية لاستخدام الأجهزة الموجودة
- التأثير التجاري عند تلف البنية الأساسية
- نقاط عدم التحصين المشتبه بها في البنية الأساسية

وفيما يلي توضيح لهذه العناصر

تعريف البنية الأساسية لاستخدام أجهزة الشبكة

قبل وضع أي خطة يجب أن تعد قائمة جرد بأجهزة الشبكة الموجودة بالشركة يجب أن يعرف مدير الشبكة جيداً عدد وحدات الخدمة وعدد محطات العمل وباقي أجهزة الشبكة مثل الطابعات.

ليس ذلك فقط، بل يجب الاحتفاظ بقائمة الجرد هذه في مكان آمن بعيد عن موقع الشبكة لأن في حالة كارثة مثل الحريق ستضيع قائمة الجرد مع موارد الشبكة . يجب أن يعرف

مدير الشبكة أيضاً البنية الأساسية للشبكة بما في ذلك الموظفين بالإضافة إلي قائمة الجـــرد المفضلة، يجب إنشاء خريطة مفصلة للشبكة ، والاحتفاظ بجميع الوثائق التي تحوي بيانات عن الشبكة، والكيفية التي يجب أن يتم العمل بها. يحتاج هذا العمل إلي مدير شبكة أو فريق عمل يفهم جيداً بنية الشبكة وكيفية وضع الخريطة. هناك برامج تقوم بمهمة إنشاء خرائط الشبكة مثل **Microsoft**.

تقييم التأثير التجاري عند وقوع الكارثة

يجب علي مدير الشبكة أن يقيم الوقت الذي يمكن أن تظل المؤسسة تعمل فيه دون تـــوفر النظام الأساسي، وما هو التأثير التجاري الذي ستتعرض له المؤسسة. وما هو التأثير والقرار إلي سيحدث في حالة تعطل قاعدة بيانات تحتفظ بسجلات الموردين أو العملاء.

تقييم نقاط عدم التحصين لبنية الشبكة

إن تعريف نقاط عدم التحصين يعد استكشاف لمشكلات الشبكة وإصلاحها قبل حـــدوث المشكلة (سوف نناقش مشكلات الشبكة وإصلاحها في الفصل القادم)

أهم ميزة في إجراء تقييم لنقاط عدم التحصين في الشبكة، أن مدير الشبكة يمكن إصـــلاح بعض الأمور التي من المحتمل أن تحدث مشكلات قبل أن تقع الكارثة .

وكمثال علي نقطة عدم التحصين: إذا كانت الشركة تتصل بأحد الموردين من خلال اتصال **WAN** واحد. يمكن إغلاق نقطة عدم التحصين هذه أو تقليلها إلي أدنى حد عـــن طريق إنشاء اتصال متكرر بالمورِّد

تطوير خطة الاسترداد

بعد الانتهاء من تقييم بنية أجهزة الكمبيوتر والتأثير التجاري للكارثة وفهم نقـــاط عـــدم التحصين، يجب أن يبدأ مدير الشبكة أو فريق العمل في تطوير الخطة المناسبة للاسترداد من الكوارث. نوضح فيما يلي بعض الأمور الهامة والتي نعتقد أنها ذات فائدة عند وضع خطط الكوارث. رغم أن الكوارث تتعدد ولكل منها خطة معينة، فإن هناك معلومات أو عناصر مشتركة في معظم خطط الكوارث هي:

- يجب أن تشمل الخطة على معلومات عن كيفية الاتصال بالموظفين الأساسيين في حالة وقوع كارثة
- يجب أن تشمل الخطة علي معلومات اتصال لكل من الموردين والعملاء المهمين.
- معلومات تأمين الشبكة مثل أسماء المستخدمين وكلمات مرورهم
- موقع معلومات النسخ الاحتياطي مثلاً أن توضع شرائط النسخ الاحتياطي وغيرها من معلومات الشركة
- يجب أن يكون هناك مكان معروف يلتقي فيه كل الموظفين كفرع الشركة أو مكان آخر في حالة الكوارث التي تجعل موقع الشركة غير قابل للاستخدام.

إنشاء مكتبة

بصفتك مدير للشبكة فأنت المسئول الأول عن حل المشاكل التي يواجهها المستخدمون للشبكة وعادة يتوقع أن يجدوا عندك حلا لجميع المشاكل التى يواجهونها مهما كان نوعها. ويتوقعون أن تكون علي خبرة بجميع البرامج التي يعملون عليها ولأن هذا الأمر صعب التحقيق ، فان الحل يتمثل فى إنشاء مكتبة كمبيوتر تتوافر بها جميع المعلومات التى تحتاج إليها فى حل أى مشكلة قد تواجهك .

وفيما يلى بعض المصادر التى يمكنك الاسترشاد بها لإنشاء مكتبة .

- نسخة من معلومات الشبكة التى قمت بتسجيلها والمتضمنة لجميع المعلومات المتعلقة بتهيئة الشبكة .
- نسخة إرشادات الاستخدام لكل برنامج على الشبكة
- مجلة واحدة على الأقل تتناول الكمبيوتر بصورة عامة ، وأخرى مخصصة لمستخدمي الشبكات ، حتى تكون لدى المكتبة معلومات عامة عن تطورات مجال الكمبيوتر بأكمله وتطورات الشبكات بصورة عامة .
- معلومات وافية عن النظم التى تستخدمها فى شبكتك (يمكن الحصول عليها مثلا من الرسائل الإخبارية على البريد الالكتروني) .

استشارة الخبراء

من الطبيعي أن تحتاج لاستشارة من هو أكثر منك علماً أو خبرة بل ربما تلجأ لاستشارة من هو أقل منك علماً وخبرة لدرايته بموضوع السؤال.

إذا اضطررت إلي هذه الاستشارة، ضع في اعتبارك عدة أمور منها :

- فكر جيداً في المشكلة التي تواجهك. ربما تصل إلي حل مناسب لها. الجأ إلي خبير في المسائل التي تعجز عن التصرف فيها بعد بذل أقصي جهد ممكن.
- إذا لم تجد من هو أكثر منك خبرة في مجال السؤال سواء كان عن الكمبيوتر عموماً أو الشبكات خصوصاً ، التحق بمجموعة متخصصة في برنامج الشبكة التي تستخدمه أو اتصل بخبراء الكمبيوتر علي الانترنت.
- ابدأ بمطالعة المجموعات الإخبارية المتنوعة بمجال الكمبيوتر أو الشبكات علي شبكة الانترنت، أو اشترك في الرسائل الإخبارية المتعلقة بمجالك.

ملخص الفصل

في هذا الفصل ناقشنا الأمور التي تساعد مدير الشبكة في إدارة شبكته والمحافظة علي استمرارها في العمل بشكل جيد. وقد ناقشنا أهم هذه الأمور ومنها مواكبة تطورات تكنولوجيا المعلومات وترقية الشبكة لتساير أحدث تكنولوجيا في الشبكات ومنها أيضا نسخ البيانات احتياطياً والتخطيط للاسترداد من الكوارث حتي لا تضيع البيانات إذا حدث لا قدر الله ووقع المحظور. ناقشنا أيضا أمور أخري تساعد علي تسير العمل قبل إنشاء مكتبة واستشارة الخبراء.

تدريبات

١. أذكر أنواع النسخ الاحتياطي؟

٢. ضع علامة (✓) أمام العبارة الصحيحة وعبارة (✗) أمام العبارة الخاطئة.

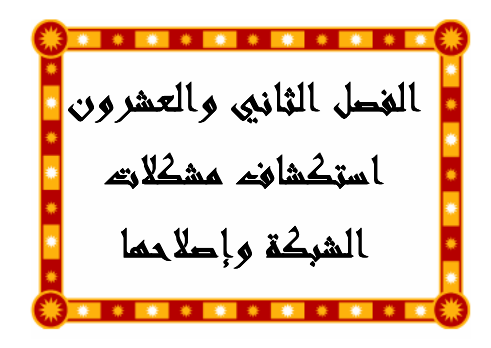
أ. من الضروري وضع خطة استرداد من الكوارث للشركات الصغيرة.

ب. يغني سجل معلومات الشركة عن وجود مكتبة متخصصة.

ج. يجب علي مدير الشبكة تقييم التأثير التجاري عند وقوع كارثة.

د. يجب علي مدير الشبكة فهم نقاط عدم التحصين في بنية شبكته.





تواجه أفضل الشبكات تصميماً وتوصيفاً مشكلات، بعضها قد يتعلق بالاتصال بالشبكة أو في الوصول إلي خدمات الشبكة المهمة. في هذا الفصل سوف نلقي نظرة علي بعض الأدوات وعمليات التفكير التي تساعد في عملية استكشاف مشكلات الشبكة وإصلاحها. بانتهاء هذا الفصل ستتعرف علي :

- *فهم العطل وإصلاحه.*
- *توقف الجهاز وتحديد سبب العطل.*
- *فحص كابلات الشبكة.*
- *مراقبة وحدة الخدمة.*
- *استخدام سجلات الأحداث.*
- *رسائل الإعلام عن الخطأ.*

إن البنية التى ترتكز عليها الشبكات تسمح بحدوث أخطاء ، نظرا للكم الهائل من الكابلات و الموصلات والكروت المستخدمة فيها . ولأن الأعطال التي يمكن أن تحدث للشبكة كثيرة . فإننا سنركز في هذا الفصل على مشكلات الشبكة الشائعة التى يمكن للمستخدم العادي التعامل معها . كما نرشد المستخدم إلي التصرف السليم فى حالة حدوث عطل يعجز عن إصلاحه بنفسه .

حاول أن تتفهم العطل و تصلحه بنفسك

من المهم أن تحدد سبب العطل فى الشبكة . تحديد العطل يساعدك فى حل المشكلة. قد تكون المشكلة فى جهازك وقد تكون المشكلة فى الشبكة . إذا كانت المشكلة عدم القدرة على الوصول إلي أجهزة الشبكة المشتركة مثل الطابعة أو محركات أقراص الشبكة ، فحاول أن تصل إلي أى منهما من أى جهاز آخر فى الشبكة . إذا لم تتمكن ، فهذا معناه أن المشكلة فى الشبكة نفسها . أما إذا كنت أنت الوحيد الذى لا يمكنك الوصول إلي الطابعة أو محرك القرص مثلا فهذا معناه أن المشكلة تكمن فى جهازك فقط . وأن المشكلة ليست لها صلة بالشبكة .

فيما يلى بعض الأفكار التى قد تساعدك فى تحديد الأعطال البسيطة إذا توقف جهازك بالكامل ومن ثم إصلاحها بنفسك قبل أن تلجأ إلي فريق الصيانة .

- تأكد إن الجهاز الذي تعمل عليه وجميع المكونات التى يشتمل عليها مثبته جيدا فعدم تثبيت كابلات الجهاز يعوق تشغيل الجهاز و يعتبر واحدا من أهم أسباب أعطال الكمبيوتر
- تأكد أن جهازك متصل جيدا بالشبكة .
- راقب رسائل الخطأ التى قد تظهر على الشاشة . إذا كان جهازك متصلا بجهاز تثبيت التيار أو بمصدر الطاقة، فتأكد أن وصلات هذين الجهازين مثبته جيدا وأنهما فى وضع التشغيل .
- استعن ببرنامج **Windows Networking Troubleshooter** .

- أعد تشغيل الجهاز والجهاز الخادم إذا لزم الأمر.
- إذا استمرت المشكلة بعد اتخاذ الخطوات السابقة ،لابد من الاستعانة بقسم الصيانة .

توقف الجهاز وتحديد سبب العطل

إذا توقف الجهاز بالكامل عن العمل فيجب عليك التحقق من بعض الأمور البسيطة قبل استدعاء فريق الصيانة أو أحد أفراده منها:

- فحص الكابلات للتأكد أنها مثبتة جيداً .
- تأكد أن وصلات مصدر الطاقة أو مثبت التيار مثبتة جيداً ، وأنهما في وضع التشغيل (إذا كان للجهازين أو أحدهما لمبة إضاءة تأكد أنها مضاءة) .
- قد يكون الجهاز في وضع **Sleep** (النوم). وفي هذه الحالة يبدو الجهاز متوقفاً في حين أنه يعمل. في هذه الحالة حرك الفأرة قليلاً .
- إذا كنت تستخدم جهاز تثبيت للتيار، راجع العمر الافتراضي لهذا الجهاز، فإذا كان تجاوز العمر الافتراضي استبدله. ربما يكون توقف الجهاز بسببه.
- تأكد أن الكابل الواصل بين الشاشة ومصدر الطاقة مثبت جيداً وأنها في وضع التشغيل إذا كان للشاشة مفتاح مستقل بها. أما إذا عرفت سبب العطل في جهاز الكمبيوتر وتريد أن تعرف ما إذا كان هذا العطل ناتجاً عن الشبكة أم جهازك، فيجب أن تقوم بالإجراءات الآتية التي يمكن أن تساعدك في تحديد مصدر المشكلة.

✓ إذا كانت المشكلة هي العجز عن الوصول إلي محركات أقراص الشبكة والطابعة المشتركة ، وكنت أنت الوحيد الذي تعاني من عدم إمكانية الوصول، فهذا معناه أنها تكمن في جهازك فقط. فقد يكون الجهاز عاجزاً عن الاتصال بالشبكة وقد لا يكون مهيأً بالصورة المناسبة للعمل عليها وقد لا يكون للمشكلة صلة بالشبكة. حاول أن تصل إلي محركات الأقراص أو الطابعة المشتركة من كل جهاز في الشبكة. إذا لم تتمكن فهذا معناه أن المشكلة تكمن في الشبكة نفسها ولابد من استدعاء فريق الصيانة أو أحد أفراده.

- ✓ إذا قمت بتنفيذ العملية التي تعجز عنها من جهاز آخر بنجاح، فحاول أن تسجل الدخول إلي الشبكة من جهاز آخر باستخدام **ID** الخاص بك.

إذا استطعت أن تنفذ العملية بنجاح فغالباً ما يشير هذا إلي أن مصدر المشكلة هو جهازك، وليس وحدة الخدمة. وفي هذه الحالة يفضل استدعاء فريق الصيانة.

فحص كابلات الشبكة

تعد الكابلات واحدة من أهم مسببات المشاكل التى تسبب أعطال الشبكات . ولذلك فإننا سنوضع فيما يلى بعض المشكلات التى تنشأ بسبب الكابل .

إذا كانت الشبكة تستخدم كابل من نوع **twisted – Pair** و أردت أن تتعرف على سلامة وصلة الكابل ، فكل ما عليك هو النظر إلي الجهاز من الخلف . توجد خلف الجهاز لمبة صغيرة بجوار موضع تثبيت الكابل انظر إلي اللمبة ، فإذا كانت متوهجة باستمرار ، فهذا معناه أن الوصلة جيدة . أما إذا كانت اللمبة مطفأة أو كانت إضاءتها متقطعة فهذا معناه انه توجد مشكلة فى وصلة الكابل .

إذا كانت إضاءة اللمبة متقطعة . انزع الكابل من الجهاز ثم ادخله مرة ثانية .

إما إذا كانت الشبكة تستخدم كابل من نوع **Coaxial** ففي هذه الحالة يكون الموصل الموجود خلف جهاز الكمبيوتر على شكل حرف **T** الرئيسي بالجهاز بينما يتصل واحد او اثنان من الكابلات **Coaxial** بالإطراف الخارجية لشكل **T** .

فى حالة استخدام كابل **Coaxial** واحد ، يجب استخدام جهاز خاص يعرف باسم مقاوم طرفي عند الطرف الآخر من **T** بدلا من الكابل الأخر.

فى حالة الشبكات التي تستخدم جهاز **Hub** لتوصيل أجهزة الشبكة ، قد تحدث مشكلات فى كابلات جهاز **Hub** خاصة عندما تتداخل كابلات التوصيل للجهاز . عندما تحدث مشكلة بهذه الكابلات ، لا تتدخل والجأ إلي أخصائي صيانة .

في حالة الشبكات التي تستخدم كابل توصيل قصير . يتصل طرف هذا الكابل بالكمبيوتر والطرف الأخر بموصل للكابل مثبت بالحائط . افصل هذا الكابل وأعد تركيبه . فإذا

استمرت المشكلة ابحث عن كابل توصيل آخر لاستخدامه .

مراقبة وحدة الخدمة (الجهاز الخادم)

تقوم وحدة الخدمة بدور أساسي في الشبكة ونظراً لحساسية الدور الذي تلعبه أجهزة الخادم في الشبكة فيجب علي مدير الشبكة أن يكون مترقباً أو متوقعاً لبعض المشاكل .
إذا خططت جيداً لاحتمالات نمو الشبكة في المستقبل منذ البداية ، ستقوم بشراء جهاز الخادم بالمواصفات التي توفر الخدمات بفاعلية حتي عند زيادة عدد مستخدمي الشبكة .
توجد أدوات لتعقب أداء أجهزة الخادم . تفيد هذه الأدوات في تعقب أداء الخادم بمرور الوقت وتحديد مكوناته. مثلاً قد تصبح ذاكرة الكمبيوتر معوقا عندما لا تستطيع مجاراة تدفق البيانات مما يسبب بطء الجهاز الخادم . كما أن القرص الصلب يعد عائقاً عندما لا يستطيع استيعاب البيانات المتدفقة بالشبكة وعادة تقدم نظم تشغيل الشبكات المختلفة أنواعا مختلفة من أدوات المراقبة . ومع ذلك يجب عليك مراقبة بعض مكونات الأجهزة بمرور الوقت . وفيما يلى نوجز نوضح بعض الأدوات التى تسمح لك بمراقبة أداء وحدة الخدمة.

أداء المعالج

عادة تشتمل أجهزة الخادمات على معالجات سريعة .والمشكلة التي يمكن أن تحدث بسبب أداء الخادم عندما تكون سرعة المعالج بطيئة بحيث لا يستطيع الجهاز الخادم مجاراة كل الاتصالات التى يحصل عليها من عمليات البرامج التى يتم تشغيلها على الخادم .
وتزودك معظم نظم تشغيل الشبكات بنوع من العدادات ترتبط بأداء المعالج .
يوفر **Windows Server 2003** على سبيل المثال عدادات يمكن عرضها لمراقبة أداء المعالج وإعداد الخطوط المبدئية لجهاز الخادم . يتم عرض هذه العدادات باستخدام . **Windows Performance Monitor** أو مراقب أداء **Windows** وهذا المراقب يمكنك من عرض أداء المعالج وجهاز الخادم فى تنسيق رسم بياني
إذا تأكدت أن الخادم هو السبب في إبطاء الشبكة فيجب عليك ترقيته بمعالج أسرع أو استبداله أو إضافة معالج آخر إلي الجهاز .

حاول من البداية أن تختار جهاز خادم للشبكة قابل لإضافة اثنين أو ثلاثة من المعالجات حتى يحقق أداء أفضل .

أداء محرك القرص الصلب ***Hard Disk Performance***

يجب أن يلبى أداء محرك / محركات الأقراص الصلبة وكذلك المساحة المتوفر عليه حاجة المستخدمين لتخزين الملفات التي ينشئونها ، يجب تجهيز الخادمات بمحركات أقراص عالية الأداء .

فيما يتعلق بمحركات أقراص الخادم ، يجب عليك مراقبة الوقت الذي يقضيه الخادم بوظائف القراءة / الكتابة ، والمساحة الفارغة على القرص.

يجب أن تراقب مقدار المساحة الفارغة على محركات أقراص الخادم ، فإذا وجدت – على سبيل المثال – أن محرك الأقراص يمتلئ بسرعة . سوف تحتاج لاتخاذ إجراء معين مثل زيادة حجم وحدة تخزين معينة أو فرض قيود على المساحة التي تخصصها لمستخدمي الشبكة . احرص على استخدام أسرع محركات الأقراص المتاحة فى الجهاز الخادم . استخدم محركات أقراص **SCSI** إن أمكن .

تتصل جميع الأقراص الصلبة بجهاز الكمبيوتر من خلال كارت تحكم . وأحيانا يكون هذا الكارت هو مصدر البطء في الجهاز وليس الجهاز نفسه . احرص علي اقتناء كارت تحكم من النوع الجيد لأنه يؤثر في الأداء تأثيرا كبيراً. من الأفضل استخدام كارت تحكم منفصل لكل قرص صلب .

هناك أنواع متعددة من الأقراص الصلبة مختلفة الكفاءة وفيما يلي الأنواع الشائعة منها :

- **IDE** : اختصاراً لعبارة **Integrated Drive Electronics** هذا النوع هو الذي كان مستخدماً حتي وقت قريب وكان يتسم بسعة وسرعة أكبر . يعرف هذا النوع بأسماء أخري مثل **EIDE** أو **ATA** . ولكننا لا ننصح باستخدام هذا النوع من الأقراص الصلبة في خادمات الشبكات (يضاف **Sata**)
- **SCSI** : تنطق هكذا " سكزي" وهي اختصار لعبارة **Small Computer**

System Interface . وهي أفضل بكثير من النوع IDE الذي شرحناه قبل قليل . ولكنها أزيد في السعر عنها وظهر نوعان من هذا النوع أحدث وأسرع . الأول Fast SCSI ويعمل بضعف سرعة SCSI والثاني Fast Wide SCSI ويعمل بضعف سرعة Fast SCSI (أي أربعة إضعاف SCSI) . إذا كنت تريد أداء مرتفع الجودة للجهاز الخادم . استخدم أقراص SCSI الصلبة

أداء الذاكرة RAM Performance

عند التخطيط لشراء جهاز خادم ضع في اعتبارك أن تشتري ذاكرة أكبر مما تتطلبه المواصفات التي تزودك بها الشركة المنتجة لنظام تشغيل الشبكة . حيث أن الشركات المنتجة لنظم تشغيل الشبكات توضح لك الحد الأدنى من الذاكرة المطلوبة .

إذا كان حجم الذاكرة التي يستخدمها الخادم أقل من المطلوب، سوف يقوم الجهاز بنقل بعض العمليات إلي محرك القرص الصلب حتي ينتهي من انجاز المهمة التي يقوم بمعالجتها، ثم ينقل البيانات من محرك القرص الصلب إلي الذاكرة لكي يتمكن من معالجتها . تسمي هذه العملية أي ترحيل البيانات مؤقتاً إلي القرص الصلب انتظاراً لدورها لأن الذاكرة مشغولة بعملية أخري، تسمي Virtual Memory (ذاكرة ظاهرة أو تخيلية)

العيب في هذه التقنية أنها تسبب بطء في الخادم وتصبح نقطة إعاقة محتملة علي الشبكة.

يمكنك معالجة هذه المشكلة عن طريق إضافة المزيد من الذاكرة Ram إلي وحدة الخدمة خاصة في ظل انخفاض تكلفة الذاكرة حالياً كلما زاد حجم ذاكرة وحدة الخدمة كلما كان ذلك أفضل . احرص أيضا علي استخدام أسرع نوع من الذاكرة تدعمه اللوحة الأم (Mother Board) لجهازك .

كروت الشبكة

احرص علي شراء كروت الشبكة من النوع الجيد لأن الأنواع الرخيصة تسبب مشاكل في أجهزة الخادم التي تدعم عدداً كبيراً من المستخدمين خاصة أن أجهزة الخادمات تتعامل مع موارد الشبكة بصورة أكبر من الأجهزة التابعة.

تحتوي جميع نظم التشغيل علي خيارات تهيئة تقوم أنت باختيارها بنفسك. يجب أن تعرف

ما هي الخيارات المناسبة والتي تعبر عن أفضل تهيئة للجهاز الخادم قد تؤثر الخيارات الغير مناسبة بشكل هائل علي الشبكة

تحسين أداء الشبكة

فيما يلي اقتراحات أو أفكار لتحسين أداء الشبكة والتغلب علي البطء الذي قد يواجهك أثناء عملك .

- **أوجد طريقة لاختبار أداء وظيفة معينة من وظائف الشبكة . فإذا كنت ترغب على سبيل المثال في زيادة سرعة الطابعة فى الشبكة ، استخدم ساعة توقيت لحساب الوقت المستغرق فى طابعة المستندات**
- **قم بتعديلات فى تهيئة الشبكة ثم اعد الاختبار . فمثلا إذا كنت تعتقد أن زيادة حجم الذاكرة Ram قد يحسن من الأداء ، فقم بذالك ،ثم اعد تشغيل الجهاز الخادم وقم بإجراء اختبار الكفاءة .ثم لاحظ التغير الذي يحدث على الأداء . واتبع نفس الطريقة مع كل عنصر من عناصر الشبكة ترغب فى تحسين أدائه.**

  ولكن ضع فى اعتبارك ما يلى عند قيامك بإجراء التعديلات وإعادة الاختبار

- ✓ **اختبر كل عنصر من عناصر الشبكة على حده كلما أمكن . بمعنى آخر . قم بإلغاء التعديلات التى أجريتها على جميع العناصر التى سبق أن اختبرتها قبل البدء فى إجراء الاختبار للعنصر الجديد .**
- ✓ **سجل نتائج كل اختبار ، ليكون لديك سجل دقيق بتأثير كل تغيير تقوم بإجرائه على أداء الشبكة**
- ✓ **لا تجر أكثر من تعديل فى الاختبار الواحد . إذا قمت بإجراء أكثر من تعديل لن تعرف أي من التعديلات هو المسئول عن تغيير الأداء .**
- ✓ **أوقف أي تعامل مع الشبكة أثناء إجراء الاختبار فقد تؤثر أفعال مستخدمي الشبكة على نتائج الاختبار**

سجلات الأحداث Event Records

استخدام سجلات الأحداث لتعقب المشكلات يعتبر أداة أخري مفيدة لمدير الشبكة لتعقب مشكلات وحدة الخدمة. يساعد عرض هذه السجلات علي الوقاية من الوقوع في المشكلة لأن عرض السجلات بصفة دورية ينبه مدير الشبكة إلي احتمالات الخطأ، كما أنه يساعد بصفة دورية علي التخلص من المشكلة من البداية حتي عندما لا يتم الإبلاغ عن مشكلة أو تصبح المشكلة واضحة علي الشبكة.

في كثير من الحالات يمكن توصيف السجلات لجمع معلومات محددة مرتبطة بوحدة الخدمة. وعادة توفر نظم تشغيل الشبكات عدداً من أنواع سجلات الأحداث المختلفة. فعلي سبيل المثال تتعقب سجلات النظام أحداث مرتبطة بخدمات وموارد النظام، وتسجل سجلات التطبيقات الأحداث المرتبطة بالتطبيقات التي يتم تشغيلها علي وحدة الخدمة، بينما تسجل سجلات التأمين الأحداث المرتبطة بسلوكيات المستخدمين مثل عمليات الدخول الفاشلة أو تدقيق وصول المستخدمين إلي وحدة تخزين معينة.

يجب أن يكون مدير الشبكة علي دراية ومستوي يمكنه من تعقب سجلات النظام وأن يكون لديه قدرة علي فهم ما ينظر إليه. لأن كل نظام تشغيل له طريقة مختلفة لتسجيل أحداث السجل ثم تحديدها. يجب أن يطلع مدير الشبكة علي وثائق تشغيل الشبكة جيداً ليكتسب فهماً لما يستلزمه متابعة السجلات.

يوفر نظام تشغيل الشبكات **Windows Server 2003** أداة **Event Viewer** "عارض الأحداث" التي تسمح لمدير الشبكة بتعقب الأحداث المضمنة في سجل تطبيق وسجل تأمين وسجل نظام. تستخدم الأداة **Event Viewer** نظام رموز (**Icons**) يساعد علي تحديد ما إذا كان هناك حدث خطأ علي وحدة الخدمة أم لا. علي النحو التالي:

- رمز **Information** "معلومات" يشير إلي تسجيل أحداث النظام الناجحة والعمليات الأخرى.
- رمز **Warning** "تحذير" يعرض خطأ بسيطاً علي النظام.
- رمز **Error** "خطأ" يشير إلي خطأ في وظيفة رئيسية.

رسائل الإعلام بالخطأ

رسائل الإعلام بوجود أخطاء ذات فائدة كبيرة للمختصين في إصلاح مشكلات الشبكة . إذا ظهرت أمامك على الشاشة رسائل إعلام بوجود خطأ عند فتح جهازك ، قم بتسجيلها تمهيدا لعرضها على المختصين من فريق الصيانة .وننبهك إلي أنه قد يظهر لك عدد كبير من رسائل الإعلام بالخطأ . هذه الرسائل لا تعنى بالضرورة أن المشكلة كبيرة . ربما تكون المشكلة بسيطة ولكنها تسبب كل هذا الكم من الرسائل .

إذا كانت الرسائل تتحرك بسرعة لا تستطيع منها قراءتها ، اضغط مفتاح **Pause** أو مفتاح **Ctrl +S** لتتوقف حركة الرسائل وتتمكن من قراءتها .

وعندما تنتهى من القراءة اضغط مفتاح **Pause** مرة أخرى لاستئناف طباعة الرسائل على الشاشة .إذا لم تنتبه إلي رسائل الإعلام بالخطأ عند فتح الجهاز . أغلق الجهاز ثم أعد فتحه لقراءتها

ملخص الفصل

في هذا الفصل ناقشنا الكثير من الأمور التي تلزم لإدارة الشبكة فقد ألقينا نظرة علي الأمور التي يمكن استخدامها لمساعدتك في تحديد المشكلات التي تواجه أجهزة وبرامج الشبكة. ومشكلات اتصال الشبكة بصفة عامة وتشخيصها، يجب أن تستخدم بيانات مراقبة وحدة الخدمة بمرور الوقت لتحديد المعلومات المحتملة. يسمح لك استخدام سجلات الأحداث بتحديد المشكلات المحتملة عند حدوثها.

تدريبات

١. ماذا تفعل بصفة مبدئية إذا توقف الجهاز الذي تعمل عليه ولم تجد شخص متخصص في الصيانة لإصلاح العطل؟

٢. أذكر العناصر التي تساعد في مراقبة وحدة الخدمة.



الباب الثامن
أمان الشبكات



تمثل الشبكة خطراً أمنياً هائلاً علي بياناتك، يتمثل في قدرة أي شخص علي اختراقها إذا نجح في الوصول إلي أي جهاز علي الشبكة. لذلك فإن تأمين الشبكة أمر غاية في الأهمية. إذ بدونه لا وجود لشبكة . بانتهاء هذا الفصل ستتعرف علي :

- *لماذا نحتاج لتأمين الشبكة*
- *نظام حسابات المستخدمين*
- *حماية كلمة المرور*
- *حماية الشبكة من الفيروسات*
- *حماية الشبكة من الهجمات الخارجية*

في الماضي كان تأمين الشبكات يقتصر علي تأمين كلمات المرور الخاصة بمستخدمي الشبكة وتحديد صلاحيات للمستخدم في الوصول إلي الموارد المشتركة . أما بعد انتشار الانترنت فقد أصبحت معظم المخاوف الأمنية مصدرها الأساسي مرتبطاً بالهجمات الخارجية

من أشهر أنواع الهجمات الخارجية اختراق الهاكرز للشبكة الداخلية (توجد وسائل كثيرة لاختراق الهاكرز للشبكة أشهرها اكتشاف الهاكرز عنوان IP لنظام داخل النظام التأميني) أو إرسال رسائل الكترونية مرفق بها نوع من الفيروسات القصد منها تدمير البيانات الموجودة علي الشبكة .

ولذلك أصبح تأمين الشبكة من كل من المستخدمين الداخليين للشبكة والهجمات الخارجية للشبكة أمراً يشغل بال مدير الشبكة لأنه قد يؤدي إلي السطو علي البيانات أو تدميرها .

وفيما يلي نتناول هذه الأمور بشئ من التفصيل

تأمين الشبكة

نقصد بتأمين الشبكة أن يقوم مدير الشبكة بواحد من اثنين . إما أن يقوم بمنح صلاحيات وصول لجميع المستخدمين لكل موارد الشبكة ثم يضع قيودا على الموارد التي لايرغب في الوصول إليها أو يضع نظاما يمنع الوصول إلي جميع الموارد ثم يعطي صلاحيات لمستخدمين بعينهم للوصول إلي الموارد التي يحتاجون إليها .

من المهم جداً تعيين اسم مستخدم وكلمة مرور لتسجيل الدخول إلي الشبكة . ويتحكم مدير الشبكة في تعيين أسماء المستخدمين وكلمات المرور لكل منهم . وهنا لابد أن يجتهد مدير الشبكة لوضع مجموعة من القواعد عند تعيين أسماء المستخدمين وكلمات المرور حتي لا يمكن تخمينها من قبل أي شخص يريد السطو علي حساب مستخدم ما للوصول إلي الشبكة .

وفي النظام الأول تكون البيانات المطلوب تأمينها محددة (مثلاً ملف قاعدة بيانات الموظفين) بينما تكون باقي البيانات متاحة لمستخدمي الشبكة. وفي النظام الثاني يتم تحديد مستوي وصول لكل مستخدم علي الشبكة. فمثلاً قد يحتاج بعض المستخدمين إلي القدرة علي

قراءة ملف الموظفين علي الشبكة . في هذه الحالة يتم منح هؤلاء المستخدمين فقط إذناً أو حق قراءة هذا الملف .

نظام حسابات المستخدمين Users ID

المقصود بحسابات المستخدمين هنا حقوق دخولهم إلي الشبكة . تعمل حقوق دخول المستخدمين أو الحسابات المخصصة لهم علي قصر الدخول إلي الشبكة علي المستخدمين المصرح لهم فقط بذلك، بدون وجود حق الدخول هذا ، لا يمكن للمستخدم تسجيل الدخول إلي الشبكة .

لا يتم تسجيل دخول المستخدم إلي الشبكة إلا بإدخال ID والمقصود بـــــ ID أسماء المستخدمين ويتم تعيين أسماء المستخدمين من قبل مدير الشبكة ويجب أن يختار أسماء يسهل تذكرها (مثلاً اختيار الأحرف الأولي والأخيرة من اسم المستخدم) كما يجب مراعاة اصطلاحات التسمية التي يحددها نظام التشغيل المعمول به علي الشبكة . حيث يختلف عدد الأحرف التي يمكن استخدامها لإنشاء اسم مستخدم من نظام تشغيل إلي آخر ولذلك يجب أن يكون مدير الشبكة علي دراية باصطلاحات التسمية قبل أن يقوم بإنشاء حسابات المستخدمين

لا يقتصر دور مدير الشبكة علي تعيين أو تعريف مستخدمي الشبكة بل يمكنه التحكم في حسابات المستخدمين أو حقوق الدخول كما يلي

- **يستطيع أن يمنح صلاحيات لمستخدمين معينين بالدخول إلي الشبكة في أوقات معينة . وبذلك يستطيع أن يقصر دخول الموظفين علي الشبكة خلال ساعات الدوام الرسمي فقط .**
- **يستطيع إنشاء حقوق دخول المجموعة . وفي هذه الحالة يكون لجميع المستخدمين التابعين لنفس المجموعة جميع حقوق الوصول الممنوحة للمجموعة .**
- **يتم من خلال حقوق الدخول لمجموعة التحكم في حقوق دخول المستخدمين . مثلاً يمكن إنشاء حق دخول لمجموعة تسمي الحسابات وحق دخول لمجموعة قسم المبيعات ويخصص لكل مجموعة الملفات التي تخصها فقط بحيث لا تتداخل ملفات القسمين معاً.**

- في حالة وجود مستخدم يتطلب عمله الوصول إلي معلومات قسمين (مثلا قسم الحسابات وقسم الإدارة) يمكن أن يجعل مدير الشبكة هذا المستخدم عضواً في المجموعتين . وبالتالي يكتسب الحقوق الممنوحة لكل مجموعة ينتمي إليها .

كلمات المرور Passwords

يعد استخدام كلمات المرور أهم عامل فى تأمين الشبكة . لان أسماء المستخدمين (IDs) لا تتوفر لها السرية الكاملة حيث يتطلب العمل فى كثير من الأحيان أن يعرف كل مستخدم أسماء المستخدمين الخاصة بغيره . فعلى سبيل المثال عندما ترغب فى إرسال رسالة الكترونية إلي احد المستخدمين لابد أن تكون تعرف الاسم (ID) المخصص له .

ولهذا تعتبر كلمات المرور الوسيلة الوحيدة لمنع أي محاولة تسلل إلي الشبكة باستخدام الاسم المخصص لأحد المستخدمين ولهذا يجب استخدام كلمات مرور قوية. وكلمة المرور القوية هى كلمة المرور التى ليس من السهل أن يخمنها أي شخص ليتمكن من السطو على حساب المستخدم ويحاول الوصول إلي الشبكة .

وفيما يلى مجموعة من القواعد التى تساعد مدير الشبكة فى إنشاء كلمة مرور قوية

- لا تختار كلمة مرور يمكن تخمينها بسهولة كاسمك أو اسم طفلك أو اسم شركتك.
- اختر كلمة مرور تحتوى على مزيج من الحروف الأبجدية والأرقام .
- استفد مما تنتجه اغلب نظم التشغيل من وضع تاريخ انتهاء العمل بكلمة المرور . إذا قمت بتحديد مدة انتهاء العمل بكلمة مرور بعد أسبوعين ، يجب على المستخدم تغيير كلمة المرور بعد انقضاء هذه المدة . رغم أن هذه العملية تسبب نوعا من الإزعاج لكنها تحميك من شخص ربما تلصص عليك اثناء كتابة كلمة المرور الخاصة بك .
- احذر من تجاهل عمليات التأمين الأساسية المتعلقة بكلمة المرور حتى وأن كانت الشبكة صغيرة .

حماية الشبكة من الفيروسات

لاشك أن الفيروسات من أهم الأعمال التخريبية التي تصيب أجهزة الكمبيوتر وتؤدي إلي تدمير البرامج والبيانات . ومن سوء الحظ أن عدد الفيروسات في تزايد مستمر وكلما أنتجت الشركات مضادات للفيروسات ابتكر المخربون نوعاً جديداً من الفيروسات .

تأخذ فيروسات الكمبيوتر أشكالا عديدة . منها ما ينشط عند بداية تحميل الجهاز ويؤدي إلي تخريب الأقراص ومنها ما يصيب ملفات البرامج القابلة للتنفيذ (ملفات EXE أو Com) بمجرد تشغيل الملف المصاب يتم تحميل الفيروس في الذاكرة ويؤدي إلي تدمير الملفات القابلة للتنفيذ .

من الفيروسات الخبيثة تلك التي تصيب المستندات وملفات جداول البيانات وليس فقط الملفات القابلة للتنفيذ . من الفيروسات ما يصيب برامج تشغيل الأجهزة (منها علي سبيل المثال برنامج تشغيل مشغل البطاقات) . ولهذا فان حماية الشبكة من الفيروسات امر فى غاية الأهمية وهو لا يقل عن حمايتها بالوسائل التقليدية مثل كلمات المرور وصلاحيات الاستخدام ومراقبة عمليات تسجيل المستخدمين التى شرحناها من قبل .

والطريقة الوحيدة لحماية الشبكة من الفيروسات هى استخدام برامج مضادات الفيروسات. توجد برامج كثيرة من مضادات الفيروسات تستخدم لفحص الملفات فى بداية العمل . ننصح بان تقوم بتثبيت برامج مضادات الفيروسات ليتم تشغيلها تلقائيا لتضمن القضاء على الفيروسات قبل أن يبدأ خطرها . ورغم أن هذا يبطئ العمل بعض الشيء ، إلا أن الوقت الذي ينفق فى تنظيف النظم المصابة بالفيروسات يعد وقتاً ثميناً جدا.

توفر شركة Symantec العديد من برامج مضادات الفيروسات و تعتبر من أشهر الشركات العاملة فى هذا المجال . المال الذي تنفقه فى شراء هذه البرامج لا يعد نوعاً من الإسراف. تابع الجديد دائما فى مجال برامج مضادات الفيروسات واحرص على اقتنائها وتثبيتها على أجهزتك .

أذونات الموارد

يعد تأمين الشبكة باستخدام استراتيجيات مرتبطة بحسابات المستخدمين وكلمات المرور طريقة واحدة فقط لتأمين الشبكة الداخلية. ترتبط طريقة أخرى لتأمين البيانات والموارد المهمة على الشبكة بحقوق المستخدمين أو الأذونات لهذه الموارد. بعد أن يسجل مستخدم ما الدخول إلى الشبكة، سوف يحتاج عادةً إلى الوصول إلى الموارد على وحدة خدمة الملفات أو الطباعة. يرجع أمر تحديد مستوى الوصول الذي سوف يتوفر لكل مستخدم إلى اشتراك ما أو وحدة التخزين على وحدة خدمة الملفات إلى مدير الشبكة. يوفر كل نظام تشغيل طريقة لتعيين إذن (أو حقوق) للمجلدات أو الأدلة على خادمات الشبكة.

على الرغم من أنه من المناسب منح كل المستخدمين نفس الوصول إلى أي مورد، فإنك سوف تحتاج إلى الوضع في الاعتبار حقيقة أن كل مستخدم سوف يتطلب مستوى وصول مختلف إلى مورد معين، لا يحتاج كل شخص على الشبكة إلى حقوق أو أذونات الكتابة والتعديل . على سبيل المثال: سوف يحتاج المحاسب إلى القدرة على تحرير جداول البيانات على وحدة الخدمة، بينما يحتاج المساعد الإداري إلى القدرة على عرض البيانات المضمنة في الملف أو قراءتها . على الرغم من ذلك، يعد الحفاظ على تعيين أذونات مستقلة لكل مستخدم للوصول إلى كل مورد عملية منظمة، أمراً مستهلكاً للوقت ومرهقاً.

إن ما يميز نظم تشغيل الشبكات أنك يمكنك إنشاء مجموعات ثم تعيين أذونات أو حقوق وصول للمجموعة. بعد ذلك، سوف تحدد عضوية المجموعة مستوى الوصول الذي يحصل عليه المستخدم لموارد معينة.

على الرغم من أن حقوق الوصول لا تبعد "الهاكرز" عن الشبكة الداخلية بالضرورة، فإنها تسمح لك بتقليل التلف الذي يمكن أن يحدثه مستخدم مهمل على ملفات البيانات المهمة، أو مستوى الوصول الذي سوف يحصل عليه الهاكر إلى مورد معين عندما يستولي على حساب مستخدم معين.

حماية الشبكة من الهجمات الخارجية

تأتى الهجمات الخارجية عادة للأجهزة المتصلة بالانترنت . بعد أن أصبح الاتصال بالانترنت ضرورة . أصبح بروتوكول TCP/IP هو البروتوكول القياسي للشبكة . ولكن للأسف لم يتم وضع التأمين فى الاعتبار عند تصميم هذا البروتوكول . تمثل بروتوكولات TCP/IP والشبكة ونظم تشغيل الجهاز التابع تغيرات ممكن أن يستغلها الهاكرز الذين يراقبون اتصال الشبكة غير المؤمن عبر الانترنت . لذلك وجد الهاكرز مجموعة من الأساليب الفنية للتحايل على استراتيجيات تأمين الشبكة.

ولكن كيف يتم حماية بيانات الشبكة من قبل الهاكرز لا المخربين ؟

هناك طريقتان لحماية الشبكة .

الاولى : استخدام النظم التأمينية الثانية : استخدام تأمينIP

أولا : النظم التأمينية

هناك نظم تأمينية لبرامج ونظم تأمينية للأجهزة . يفحص النظام التأمينى البيانات التي تدخل إلي الشبكة أو التي تخرج منها . ويمكنه تصفية البيانات التى تنتقل بين الاتجاهين . حيث أن البيانات الداخلة إذا لم تلب قواعد معينة تم توصيفها على النظام التأمينى . لن يتم السماح للبيانات بدخول الشبكة الداخلية أو مغادرتها .

ثانيا : استخدام تأمينIP

إذا كانت الشبكة الداخلية تستخدم بروتوكول TCP/IP يكون لكل جهاز عنوان مميز . يمكن أن تقدم عناوين IP الداخلية للمخرب الماهر فرصة الوصول إلي مناطق غير مصرح بها على الشبكة . هناك تفاصيل فنية لعملية اختراق الهاكرز للشبكة باستخدام عناوين IP وهى باختصار شديد أن كل حزمة بيانات IP تحتوى على قدر كبير من المعلومات . وبعد أن يلتقط الهاكرز حزمة البيانات ، فإنه يمكنه قراءة عناوين IP التى توفر عناوين المصدر والوجهة .

ولمواجهة هذا الوضع تم تطوير نظام يسمى **IP Security** أو **IP Sec** . يقوم هذا النظام بتزويد شبكات **IP/TCP** بآلية تأمين تحتفظ بالبيانات آمنة أثناء النقل .بمعنى أن أي شخص يعترض طريق البيانات سواء على الشبكة الداخلية أو عبر اتصالات الانترنت ، لا يمكن قراءهما أو تعديلها أو إعادة تشغيلها .

ملخص الفصل

في هذا الفصل ناقشنا أموراً هامة لتأمين الشبكة باعتبارها أمراً يشغل بال مدير الشبكة. من المهم جداً أن يقوم مدير الشبكة بتعيين اسم مستخدم وكلمة مرور لتسجيل الدخول إلي الشبكة. يجب علي مدير الشبكة البحث عن أحدث برامج مضادات الفيروسات لحماية الشبكة من الفيروسات باعتبارها من أهم الأعمال التخريبية التي تصيب أجهزة الكمبيوتر وتؤدي إلي تدمير البرامج والبيانات. وناقشنا أيضاً حماية الشبكة من الهجمات الخارجية التي تأتي من الاتصال بالانترنت وذلك عن طريق اختيار نظم تأمينية للبرامج والأجهزة أو استخدام نظام **IP Security** .

تدريبات

١. يعتبر نظام حسابات المستخدمين وكلمات المرور واحدة من وسائل تأمين الشبكات. اشرح ذلك باختصار.

٢. أذكر ثلاثة من الأمور التي تساعد في إبطال الهجمات الخارجية.





في هذا الفصل ستتعرف علي مفاهيم أخري تساعد في حماية البيانات علي الشبكة. تشمل هذه المفاهيم :

- ***صلاحيات الاستخدام***
- ***احتياطات الأمان***
- ***تأمين الاتصال بالانترنت***
- ***تأمين الشبكات اللاسلكية***

صلاحيات الاستخدام

نقصد بصلاحيات الاستخدام الصلاحيات أو الحقوق التى تخص كل من المستخدمين ونظام الملفات ومدير الشبكة نفسه.

يعد تأمين الشبكة باستخدام أسماء المستخدمين (IDs)وكلمات المرور التى شرحناها من قبل طريقة واحدة فقط لتأمين الشبكة . رغم أهميتها البالغة في تأمين الشبكة حيث تعتبر خط الدفاع الأول في خطة تأمين الشبكة .

تأتي الصلاحيات الممنوحة للعاملين علي الشبكة أو حقوق الاستخدام في المرتبة الثانية بعد استخدام الاسم وكلمة المرور لكل منهم .

فيما يلي نوضح الحقوق أو الصلاحيات التي تخص كل من المستخدم والمدير ونظام الملفات الموجود علي وحدة الخدمة للشبكة.

بالنسبة لحقوق دخول مدير الشبكة لا ينبغي أن تفرض عليه قيود أمنية من أي نوع، لأنه هو المسئول عن نظام تأمين الشبكة بأكمله . بل تعتبر مسئولية تأمين الشبكة واحدة من أهم واجباته.

حقوق دخول المستخدم

تتفاوت الحقوق التي تمنح للمستخدمين . تعتمد حقوق المستخدم علي السياسة التي تضعها الشركة والحدود التي يراها مدير الشركة للمستخدمين وفيها علي سبيل المثال تغيير الوقت والتاريخ المسجلين بواسطة وحدة الخدمة أو الدخول مباشرة من خلال لوحة مفاتيح وحدة الخدمة. أو نسخ الملفات والأدلة من علي جهاز وحدة الخدمة واسترجاعها .

حقوق نظام الملفات

تحدد حقوق الملفات العمليات المسموح القيام بها من قبل المستخدمين علي الملفات حيث أنه من غير المقبول أن تصبح البيانات المتاحة لجميع العاملين علي الشبكة . فمثلاً في غالب الأحيان لا يسمح لموظفي المبيعات بمعرفة أسعار الشراء الموجودة بملف المشتريات، كما يمكن إعداد حقوق نظام الملفات للسماح لمستخدمين بعينهم بقراءة ملفات معينة بدون

صلاحيات التعديل أو الحذف .

رغم أن طريقة إدارة حقوق نظام الملفات تختلف من نظام تشغيل لآخر . إلا أن الفكرة واحدة وهي تحديد الصلاحيات الممنوحة لكل مستخدم بالوصول إلي الملفات أو المجلدات أو الأقراص والقيام بعمليات معينة عليها .

هناك ٦ صلاحيات أساسية في نظام **Windows** يمكن تحديد أي مجموعة من هذه الصلاحيات لمستخدم أو مجموعة مستخدمين بالنسبة لملف أو مجلد معين .

يوضح الجدول التالي الصلاحيات الرئيسية في نظام **Windows**

الصلاحية	الاختصار	العمليات المسموح بها
قراءة **Read**	**R**	فتح وقراءة الملفات
كتابة **Write**	**W**	فتح الملف وتعديله
تنفيذ **Execute**	**X**	تشغيل الملف
حذف **Delete**	**D**	حذف الملف
تغيير **Change**	**P**	تغيير صلاحيات الملف
ملكية **Take Ownership**	**O**	ملكية الملف

صلاحيات الملكية **Take Ownership**

راجع الجدول تجد في آخر عمود الصلاحية " صلاحيات الملكية **Ownership** " في نظام **Windows** لكل ملف أو مجلد مالك . وهو المستخدم الذي قام بإنشائه ويمكن نقل الملكية من مستخدم لآخر .

الهدف من صلاحية **Take Ownership** هو منع أي شخص من إنشاء ملف أو مجلد ثم نقل ملكيته إليك بدون تصريح منك .

لا يسمح **Windows** بنقل ملكية ملف لمستخدم آخر ولكنه يسمح بمنع مستخدم آخر حق اكتساب ملكية الملف .

وجدير بالذكر أن هذه الصلاحيات لا تطبق إلا علي الملفات أو المجلدات التي يتم إنشاؤها بواسطة نظام **NTFS**. إذا كنت تستخدم نظام **Fat** أو **Fat 32** فلن تستفيد من صلاحية

الملكية في تأمين الملفات أو المجلدات .

مراقبة تسجيل دخول المستخدمين

لا يكفي استخدام كلمة مرور قوية علي الشبكة. بل لابد من استخدام نظام لمراقبة عمليات تسجيل دخول المستخدمين علي الشبكة وعادة يسمح نظام تسجيل عمليات الدخول بتسجيل عمليات الدخول التي تتم بنجاح وتلك التي لا يقدر لها النجاح . وهذا يوفر نوع من المراقبة تتيح التعرف علي محاولات الدخول غير الناجحة، التي قد تتم من قبل شخص غير مسموح له بالولوج إلي الشبكة . وبالتالي تنبه صاحب الحساب أن حسابه تعرض للسطو . وعادة توفر نظم تشغيل الشبكة نوع من أنواع مراقبة تسجيل دخول المستخدمين علي الشبكة . فمثلاً يوجد في نظام التشغيل **Windows Server 2003** سجل يسمي **Security** يستخدم لهذا الغرض .

في نظام تشغيل الشبكة **Windows Server 2003** يتم تعقب الأحداث الفعلية باستخدام سجل **Windows Security** .

احتياطات الأمان

لاشك أن التخريب المتعمد والكوارث البيئية من أخطر عوامل تدمير البيانات . ولذلك فإن وضع خطة لتأمين البيانات الموجودة على الشبكة أمر بالغ الأهمية .

ناقشنا فى الفصل السابق جوانب كثيرة من هذه الخطة شملت استخدام كلمات مرور قوية على حسابات المستخدمين. ومراقبة عمليات دخول المستخدمين والتحكم فى الأوقات التى يمكن للمستخدمين فيها الدخول إلي الشبكة. شرحنا كذلك تأمين المجلدات المشتركة والأقراص المغناطيسية باستخدام صلاحيات الاستخدام.

وفيما يلى بعض الأفكار الإضافية التى تفيدك فى تأمين الشبكة

- افرض نظاماً صارماً على كلمات المرور وتأكد من أنها تستخدم بسرية تامة .
- راقب جيدا عمليات تسجيل دخول المستخدمين على الشبكة. استفسر عن الإدخالات فى سجل دخول المستخدمين كما تستفسر عن المكالمات الهاتفية الخارجية

التى تتم بالشركة.

- تأكد تماما من أن برامج مضادات الفيروسات كافية. لايكفى وضع برنامج واحد على الجهاز الخادم. استخدم برنامج آخر على محطات العمل وآخر للنظام التأميني. إن التكلفة التى تدفعها فى هذه البرامج أقل بكثير من تكلفة تدمير البيانات التى قد تتعرض لها.
- يجب على جميع العاملين بالشركة من مستخدمين ومديرين عدم إعطاء بيانات عن المستخدمين وكلمات المرور عبر الهاتف إلا بعد التأكد من هوية المتصل لأن الهاتف وسلية غير آمنة فى الاتصالات.
- احتفظ بوسائط النسخ الاحتياطي فى مكان آمن بعيداً عن أجهزة الشبكة أو حتى بعيداً عن مقر الشركة فإن الكوارث الطبيعة مثل الزلزال أو الحريق يمكن لن تأخذ منها النسخ الاحتياطية.
- ضع فى حساباتك أنك تواجه دائما مخاطر الهجوم الخارجي الذي يمكن أن يأتى من الرسائل الالكترونية أو هجمات مباشرة من الهاكرز.

تأمين الاتصال بالانترنت

لن أعيد عليك فكرة الانترنت وفائدها وربط الشبكة الداخلية بها. هذا ليس مكان مناقشة هذه الأفكار. سأفترض أنك تعرف هذه الأمور وأن شبكتك متصلة بشبكة الانترنت وسأقصر كلامي على كيفية تأمين الشبكة فى حالة اتصالها بشبكة الانترنت.

بعد اتصال الشبكة الداخلية بالانترنت، يصبح تطبيق إجراءات وضع خطة أمنية على الشبكة بأكملها امراً حتميا. من أهم المخاطر الأمنية للاتصال بالانترنت إمكانية تسلل شخص خارجي إلي شبكتك والقيام بإعمال تخريبية.

فيما يلى بعض الاحتياطات التى تقلل المخاطر التى تتعرض لها فى حالة اتصال شبكتك بالانترنت :

- قبل تنزيل البرامج والملفات من الانترنت،تأكد من وجود برنامج للكشف عن الفيروسات على الجهاز الذى تستخدمه.

- لا تفتح ملفات أو بريد مجهول المصدر أو يحتوى على عنوان مريب. فربما يشتمل هذا البريد على فيروس. احذر من مرفقات البريد الالكتروني لأنها من أكثر وسائل انتشار الفيروسات.
- لا ترسل المعلومات السرية والهامة مثل كلمات المرور و أرقام بطاقة الائتمان عبر الانترنت لاحتمال تعرضها للسرقة. إذا كان ولابد يمكن تشفير هذه المعلومات قبل إرسالها.
- لاتسمح لأى جهاز متصل بالانترنت بتنشيط مشاركة الملفات لاتصالات TCP/IP. (لمزيد من المعلومات تابع قراءة البند التالي).

إلغاء تنشيط خاصية المشاركة لاتصالات TCP/IP

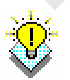
يشكل الاتصال بالانترنت من خلال جهاز مودم مخاطر أمنية شديدة . وعادة يسمح نظام Windows فى حالة وجود اتصال قائم بين جهاز كمبيوتر وشبكة الانترنت من خلال مودم بتنشيط إمكانية مشاركة الملفات والطابعة لاتصالات TCP/IP عبر جهاز مودم.

استخدام تأمين IP

شرحنا فى الفصل السابق الكثير عن إجراءات الحماية من الهجمات الخارجية وتطرقنا إلي موضوع حماية الشبكة فى حالة اتصالها بالانترنت من المخربين أو الهاكرز.

لذلك سنركز هنا استخدام تأمين IP هناك طريقة أخرى لحماية البيانات من الهاكرز الذين يحاولون الدخول إلي الشبكة باستخدام أدوات تحليل البروتوكولات، وهى استخدام تأمين IP والتشفير. يستطيع الهاكرز الحصول على قدر كبير من المعلومات باستخدام أدوات تحليل البروتوكولات لالتقاط اتصالات الشبكة غير المؤمنة.

بعد أن يلتقط الهاكرز خدمة البيانات، يمكنه قراءة رءوس عنوان IP التى تشتمل بدورها على عناوين المصدر والوجهة.



يستخدم بروتوكول TCP/IP عناوين مخصوصة تعرف باسم عناوين IP لتعريف أجهزة الكمبيوتر المختلفة المتصلة بالانترنت.عنوانIP عبارة عن رقم مكون من ٣٢ بت (أي أربعة أرقام عشرية) تنفصل عن بعضها بنقاط. تخصص لشبكتك

الأرقام الثلاثة أو الأربعة الأولى من العنوان (تبعا لحجمها) بينما يعرف بقية العنوان جهاز الكمبيوتر المتصل بالشبكة. فى حالة اتصال شبكتك بالانترنت، لا يستطيع أى جهاز على الشبكة الوصول إليها إلا من خلال عنوان **IP** الخاص به. يتم تخصيص هذه العناوين تلقائيا من خلال وحدة خدمة خاصة تعرف باسم **DHCP**. (راجع الفصل السابع عشر)

تم تطوير نظام يطلق عليه **IP Security** أو **IP Sec** ومعناها تأمين **IP**. لتزويد الشبكات التى تستخدم بروتوكول **TCP/IP** بآلية تأمين تحفظ البيانات آمنة أثناء النقل .

فإذا حاول شخص اعتراض طريق البيانات على الشبكة الداخلية أو عبر اتصالات الشبكة الخارجية فإنه لن يستطيع قراءتها أو تعديلها أو إعادة تشغيلها.

من أساليب الحماية التى يوفرها **IPSec** ضد هجمات الهاكرز أنه يقوم بتشفير البيانات على جهاز الكمبيوتر المرسل ، وهذا الأمر لا يتيح للمخرب قراءة البيانات التى يحاول اعتراضها أثناء نقلها. يقوم **IPSec** كذلك بتشفير البيانات على جهاز الكمبيوتر المستلم. وبهذا يغلق الطريق أمام الهاكرز الذي يحاول خرقها.

يدعم **Windows Server 2003** نظام **IPSec** .

تأمين الشبكات اللاسلكية

صحيح اننا لم نتعرض بعد لشرح الشبكات اللاسلكية.سيتم شرحها بإذن الله من هذا الكتاب إلا أننى فضلت مادمنا فى معرض الحديث عن تأمين الشبكات فى هذا الفصل، فضلت مناقشة بعض المفاهيم المرتبطة بتأمين الشبكات اللاسلكية.

كيف يتم اختراق الشبكة اللاسلكية

لا يلزم فى حالة الشبكات اللاسلكية أن ينجح المخرب في الدخول إلي جهاز الكمبيوتر فى شركتك حتى يخترق الشبكة ، حيث يمكن التسلل إلي الشبكات من خلال وسيلة تعرف بـــــ"التوجيه اللاسلكي". وفكرة التوجيه اللاسلكي تتلخص فى استخدام جهاز كمبيوتر محمول لاسلكي للبحث عن شبكات لاسلكية غير مؤمنة والاتصال بها .

يجهز الهاكرز أجهزتهم بهوائيات لاسلكية خارجية لتسهل لهم الحصول علي النقاط الفعالة

اللاسلكية ويلجأون في الغالب إلي استخدام جهاز يدوي يسمي **Global Positioning System** أو **GPS** وتعني (نظام تحديد مواضع عامة) لمساعدتهم في تعيين الحدود الفعلية للنقط الفعالة .

بمجرد إيجاد نقطة فعالة لاسلكية غير مؤمنة ، يستطيع الهاكرز الوصول مجاناً إلي الانترنت . بل إنهم يقومون أكثر من ذلك بإرسال معلومات عن النقاط الفعالة إلي غيرهم من المخربين الذي يستخدمون التوجيه اللاسلكي من خلال بعض المواقع علي الويب .

بل أن الأمر يصل بالبعض منهم إلي التجوال بسيارتهم في المدينة ومعهم أجهزتهم المحمولة بحثاً عن أي اتصال مفتوح بشبكة لاسلكية . وقام بعضهم بنشر خريطة طريق علي الانترنت للشبكات اللاسلكية غير المؤمنة.

يستخدم الهاكرز مصطلح **War driving** للإشارة إلي أدوات اختراق الشبكات اللاسلكية . إذا بحثت عن كلمة **War Driving** باستخدام أحد محركات البحث، ستجد الكثير من المواقع تحتوي علي عدد كبير من الأدوات للتسلل إلي الاتصالات اللاسلكية .

كيف نحمي الشبكة اللاسلكية

فيما يلي بعض الإرشادات التي قد تعينك علي حماية الشبكة اللاسلكية. تستخدم الشبكات اللاسلكية جهاز يسمي **Wireless Access Point** وتختصر هكذا **WAP** لوصل أجهزة الكمبيوتر اللاسلكية بالشبكة السلكية الموجودة بالفعل . لذلك يجب عليك تنشيط سمة **Wired Equivalent Privacy** وتختصر **WEP** لجميع الأجهزة اللاسلكية في شبكتك . تعمل سمة **WEP** علي تأمين البيانات المنقولة في الشبكات اللاسلكية . ورغم أن هذه السمة لا توفر حماية تامة للبيانات إلا إنها تمنع محاولات التسلل المعتاد إلي الشبكة .

تستخدم الشبكات اللاسلكية ما يعرف بـــ **Service Set Identifier** وتختصر هكذا **SSID** ومعناها (معرف محدد الخدمة) لتعريف الشبكة اللاسلكية . بعبارة أخري يستخدم كاسم للشبكة اللاسلكية . يتم الاتصال بنقاط الوصول للشبكة اللاسلكية عن طريق **SSID** بواسطة أجهزة وكمبيوتر محمولة .

يوصف كل مورد نقطة وصول نقاط الوصول الخاصة به باستخدام **SSID** افتراضي

ويعرف الهاكرز ماهية معرفات SSID الافتراضية لمعظم نقاط الوصول للشبكة . لحماية شبكتك قم بتغيير القيم الافتراضية SSID . ولكننا ننصحك ألا تعول كثيراً علي تغيير SSID لان التغيير لن يحمي الشبكة كثيرا.

- احذر من تثبيت أجهزة Wireless Access Point بخلاف تلك التي قمت بنفسك بتثبيتها على الشبكة. نظرا لانخفاض أسعار WAP وسهولة تثبيتها فقد يقوم احد المستخدمين بتثبيت أحدها على الشبكة بدون إذن من مديرها. قد تعرض هذه الأجهزة الشبكة بالكامل للخطر .
- قم بتغيير جميع كلمات المرور الافتراضية، خاصية كلمات مرور WAP وحقوق دخول مدير الشبكة، وذلك لجميع أجهزة وحدة الخدمة. ترجع معظم حالات فشل الخطط التأمينية لأجهزة الكمبيوتر إلي استخدام كلمات مرور غير قوية.

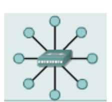
ملخص الفصل

في هذا الفصل ناقشنا كيف يمكن حماية البيانات علي الشبكة. تعتبر الحقوق التي تمنح للمستخدمين لأداء بعض الأعمال والامتناع عن البعض الآخر وسيلة فعالة لحماية بيانات الشبكة. وكذلك يجب وضع قيود علي العمليات المسموح القيام بها من قبل المستخدمين علي الملفات.

استخدام أساليب التأمين المعروفة كتأمين الاتصال بالانترنت أمر هام أيضا لحماية البيانات. ناقشنا أيضا بعض الأفكار لحماية الشبكة اللاسلكية باعتبارها أسهل الشبكات اختراقاً.

تدريبات

١. كيف يمكن تأمين شبكتك في حالة الاتصال بالانترنت ؟
٢. أذكر ثلاثة من الأمور التي نفيدك في تأمين شبكتك ؟





في الواقع ، الويب عبارة عن مجموعة من الموجهات ووحدات الخدمة التي تؤلف أكبر شبكة منطقية واسعة (WAN) في التاريخ المدون. إن مجموعة معدات التشبيك هذه كلها متصلة بالانترنت ويستطيع أن يصل إليها كل شخص متصل أيضاً.

وإذا كان كامل المعرفة البشرية مخزنة علي وسائط مغناطيسية. فإننا قلقون بشأن أمان هذه الشبكة، تمثل جدران النار واحدة من التدابير الوقائية المستخدمة لحماية هذه الكمية الهائلة من المعلومات. بالانتهاء من هذا الفصل ستتعرف علي :

- *جدار النار.*
- *ضرورة جدار النار.*
- *جدران النار كأسلوب أمان.*
- *كيف يعمل جدار النار.*
- *جدران النار أثناء عملها.*
- *أنواع جدار النار.*

هل هناك مؤسسة ما تحافظ علي النظام في الانترنت بنفس الطريقة التي تحافظ بها الشرطة علي النظام علي الطرقات العامة؟ أو هل هناك وكالة حكومية تتطفل علينا وتفحص جيداً كل جهاز موصول بالانترنت؟ الجواب علي هذه الأسئلة هو لا؛ ليست هناك مؤسسة موحدة مسئولة عن حماية الانترنت. إن وظيفة حماية والمحافظة علي مداخل قاعات المعرفة علي الانترنت متروكة للشخص (أو الأشخاص) المسئول عن نشر تلك المعلومات في المقام الأول. كل موقع ويب يتصدره اتصال شركة بالانترنت أو مزود خدمة الانترنت (**ISP**، أو المزود)، وتكون وظيفته هي التأكد أن القراصنة (الأشرار) لا يسببون فوضى في معلومات موقع الويب المخزن والمصنفة بعناية. ولكن كيف نحمي موقع ويب أو وحدة خدمة بريد أو وحدة خدمة **FTP** أو بقية مصادر المعلومات التي يمكن الوصول إليها من الويب؟ الجواب بسيط جدا: جدار نار **(firewall)** .

جدار النار

هو جهاز أمان يجلس على حافة اتصالك بالانترنت ويعمل كضابط أمن على حدود الانترنت. إنه ينظر إلى كل حركة المرور التي تدخل إلى اتصالك وتخرج منه، منتظراً حركة مرور يمكنه أن يصدها أو يرفضها وفقاً لقاعدة معتمدة. جدار النار هو القانون في ويب عالمية خالية من القوانين . إنه يقظ دائماً في مهمته لحماية الموارد الداخلية للشبكة الموصولة به.

لقد جعلت الانترنت كمية هائلة من المعلومات متوفرة للمستخدمين سواء للأفراد أو للشركات. لكن جعل معلوماتك متوفرة على الانترنت يمكن أن يعرض البيانات المهمة أو السرية لهجمات من أى مكان فى العالم _ الانترنت هي شبكة عالمية بكل ما للكلمة من معنى. وهذا يعني أنني عندما أتصل بالانترنت في جنوب أفريقيا يمكن أن أتعرض لهجوم من أوروبا أو آسيا، الخ. بإمكان جدران النار أن تحمي كمبيوترات الأفراد وشبكات الشركات من الاقتحام العدائي عبر الانترنت، لكن يجب أن تفهم جدار نارك لكي تستعمله بشكل صحيح.

هذا " الشرطي الالكتروني" الذي يعمل على مدار الساعة وفي كافة أيام السنة لديه وظيفة

مهمة جداً: إبقاء الأشرار خارجاً وتمكين الأخيار من الوصول إلي الموارد التى يحتاجون إليها ليقوموا بأعمالهم .يبدو هذا الكلام بسيطاً جداً على الورق، لكن ضبط تكوين جدار نار" بشكل صحيح" في الواقع هو أمراً ليس سهلاً .

قبل أن نشرح عمل جدار النار نورد فيما يلى بعض الأسئلة المشروعة التي توضح واجبات جدار النار لفهم ما الذي يجعله يعمل وكيف يؤدي عمله.

من يحتاج إلي جدار نار؟

إنه ربما أكثر أسئلة الأمان تداولاً.إذا كنت تنوى الاتصال بالانترنت، تحتاج إلى جدار نار. لا يهم إذا كنت تتصل من المنزل أو من شركتك. إن الانتشار المتزايد لخدمات الانترنت العريضة النطاق في المنازل وميزهّا بأنك ستكون متصلاً بالانترنت دائماً يجعل أمان المنزل أهم بكثير من ذي قبل.

لماذا أحتاج إلى جدار نار ؟

مثلما كان القراصنة في قديم الزمان يتجولون في البحار، يتجول القراصنة في ساحات الانترنت وهم يسعون إلى النيل منا. في أغلب الأحيان لا تريدهم أن يدخلوا شبكتك ويتجولوا بين الكمبيوترات الموصلة بها.

أنت تعرف أنه يجب أن تحمي شبكتك من أولئك المهاجمين، وإحدى الطرق الأكثر فعالية لحماية شبكتك هي تثبيت جدار نار. بشكل افتراضي، أي جدار نار جيد يمنع تبادل أى حركة مرور غير مرغوب فيها بين الانترنت وبين شبكتك الداخلية. وفي سياق ذلك، يزود جدار النار قواعد فحص الرزم المبين للحالة (SPI) لكل رزمة واردة.

البديل لاستخدام جدار نار هو السماح لكل اتصال بدخول شبكتك _ يعنى لن يكون هناك أي نوع من أنواع فحص الرزم لتحديد ما إذا كان هناك هجوم يختبىء ضمن إحدى الرزم الواردة أم لا. إن عدم استعمال جدار نار سيجعل مؤسستك متاحة أمام جميع المتواجدين على الانترنت .

هل لدي أي شيء يستحق الحماية؟

ربما تسأل مثل هذا السؤال :" أنا أفهم أنه لو كان لدي شيء يستحق الحماية، لكنت سأحتاج إلي جدار نار بالتأكيد. لكنني لا أملك أي شيء سيرغب به المهاجمون، لذا لماذا يجب أن أكترث لوجود جدار نار أو لعدم وجوده؟"

الشبكات ومواردها مهمة للطريقة التي ننجز بها أعمالنا الشخصية والتجارية . هذا يعني أن هناك قيمة لشبكتك ولتمكينها من أن تعمل بفاعلية. هذا الدور المتزايد للشبكات يعني أنك بالتأكيد تملك شيئاً يستحق الحماية إلى درجة ما، ويتضح ذلك مما يلي :

- *البيانات المفقودة* : ماذا لو لم تستخدم جدار نار وقام مهاجم بحذف بياناتك لأنه يستطيع ذلك؟ ماذا سيحصل للشركة؟ هل ستتكلف أموالاً لإعادة إنشاء كل شيء؟ هل ستعاني من فقدان المبيعات؟ لا شك أنك سمعت بقصص الشركات التي فقدت كل بياناتها المهنية في هجمات الفيروسات الشهيرة ، والعديد منها لم يتمكن من استعادتها.
- *تهديد البيانات السرية*: لكل مؤسسة بيانات تعتبرها سرية وفقدانها قد يسبب مشاكل مالية أو قانونية أو إحراجاً شديداً . قد تنتج تلك الأشياء عن فقدان معلومات الزبائن كأرقام بطاقات الائتمان أو وقوع الخطط السرية في أيدي المنافسين.اللائحة لا تنتهي وعندما تتعرض للقرصنة، يجب أن تفترض أسوأ الاحتمالات. لهذا السبب على الأرجح لا يتم تبليغ الشرطة عن معظم الجرائم الإلكترونية .
- *توقف عمل الشبكة*: هل ذهبت يوماً إلي الصراف الآلي أو متجر بقاله للحصول على نقود ودفعت بواسطة البطاقة في قارئة البطاقات؟ الشبكات هي التي تسمح لتلك الأجهزة بأن تعمل بشكل جيد عادة ، لكن إذا لم تكن محمية، قد يتسبب مهاجم بتعطيلها. يمكن لخسارة الإيرادات من تلك الشبكات أن ترتفع بسرعة إذا أصبحت غير متوفرة للمستهلكين. توقف العمل هو كالخراب لأى شبكة، ويتم دائماً احتساب كلفة مقترنة بهذه الأنواع من الأحداث.

في نهاية المطاف، لدى الجميع شيء يستحق الحماية، ولا ينصح بعدم فعل ذلك؛ إنها مجرد مسألة وقت قبل أن يحصل شيء. السؤال التالي هو "ما الذي يفعله جدار النار لحماية شبكتي؟"

ما الذي يفعله لي جدار النار؟

- يفحص جدار النار مرور البيانات عند دخولها إحدى واجهاته ويطبق قواعد على حركة المرور، فيسمح أو يمنع حركة المرور بناءً على تلك القواعد ، يصفي جدار النار حركة المرور الواردة والصادرة على حد سواء.
- تستطيع جدران النار أن تصفي حركة مرور بناءً على عناوين **IP** المصدر / الوجهة والبروتوكول وحالة الاتصال. بمعنى آخر، قد لا تسمح عادة بدخول **FTP** إلى شبكتك (من خلال جدار النار)، لكن إذا بدأ مستخدم جلسة **FTP** من داخل شبكتك، سيسمح للجلسة لأنها بدأت من داخل الشبكة. بشكل افتراضي، تثق جدران النار بكل الاتصالات بالانترنت من الشبكة الداخلية الموثوق بها .
- بإمكان جدار النار أيضاً أن يسجل محاولات الاتصال مع بعض القواعد التي قد تصدر أيضاً إنذاراً إذا حدثت.
- أخيراً تتيح لك جدران النار تنفيذ ترجمة عناوين الشبكة **(NAT)** من العناوين **IP** الخصوصية الداخلية إلى عناوين **IP** عمومية.

جدران النار هي " أسلوب الأمان"

إن وجود شبكة تتصل بالانترنت من خلال جدار نار هي فقط الخطوة الأولى نحو الأمان ؛ يجب أن تعرف الآن أن أساليب الأمان تشكل الأساس لكيفية استخدام تلك القواعد.

كيف يمكن لجدار نار أن يكون أسلوب الأمان ؟ المسألة بسيطة _ فجدار النار يقوم بما يفترض أن يقوم به عن طريق إتباعه " القواعد" التي ضبطها مهندس الشبكة أو رئيس أمان المعلومات **(Security Officer Information)** . يجب أن تتماشى تلك القواعد بشكل مثالي مع سرد مكتوب موجود في مستند أسلوب الأمان الذي تضعه على الرف،. يجب أن يحتوى مستند أسلوب الأمان على معلومات ولائحة بقواعد الشبكة. الشيء المثير

للاهتمام هو أن كل القواعد الواردة في مستند " أسلوب الأمان " يجب ضبطها في جدار النار أيضاً .

في محاولة لتوسيع تشبيه جدار النار بـــ "أسلوب الأمان" افحص بعض النقاط الإضافية عن أسلوب الأمان وكيف يتماشى معها جدار النار:

- يبين أسلوب الأمان ما هو الإجراء الذي سيتخذ رداً على الظروف التي تنشأ .
- إن مستند أسلوب الأمان يتطور ويتغير باستمرار ليستوفي الاحتياجات الأمنية الجديدة.
- يفض أسلوب الأمان معايير الاستخدام المقبولة وغير المقبولة.

خلاصة القول أن تقتنع أن جدار النار ليس بديل لمستند أسلوب الأمان، ولكن لجعلك تفكر بالأمان كفلسفة شاملة من خطط وأساليب وأجهزة أمان. يجب أن تبذل جهداً كبيراً في التفكير بحل متكامل _ لا أن تتكل على ناحية واحدة فقط لحماية شبكتك. عندما تصبح جاهزاً لتخطيط تكوين جدار نارك وتطور القواعد التي تسمح أو تمنع حركة المرور، يجب أن تستعمل أسلوب أمانك كنقطة الانطلاق. جدران النار هي التجسيدات المادية والمنطقية لأساليب أمانك .

كيف تعمل جدران النار

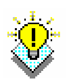
معظم جدران النار (معظمها وليس كلها) يتكل علي فحص الرزم المبين للحالة **(SPI)** لتعقب أثر كل الرزم الصادرة والأجوبة التي قد تولدها تلك الرزم. تعقب أثر المضيفات على الشبكة المحمية التي تولد الرزم الصادرة يمنع رزم الشبكة **WAN** الشريرة أو التوسلية من دخول واجهة خارجية.

بمعنى آخر، جدار النار الذي يستعمل **SPI**، يراقب كل حركة المرور التي تبدأ من مضيف داخلي، ويتعقب المحادثة من ذلك المضيف إلي الوجهة الداخلية،ويضمن أن الجواب الوارد على ذلك الطلب يصل إلي المضيف الذي بدأ العملية برمتها أصلاً .

الهدف المزدوج لفحص الرزم وتصفية الرزم هو إحدى المسؤوليات الرئيسية لجدار النار. نوضح فيما يلي القواعد والميزات الأكثر شيوعاً لجدران النار:

- ***صد حركة المرور الواردة إلي الشبكة بناءً على المصدر أو الوجهة*** _ صد حركة المرور الواردة غير المرغوب بها هو الميزة الأكثر شيوعاً لجدار النار وهو السبب الرئيسي لاستخدام جدار نار ضد الدخول. تأتي حركة المرور غير المرغوب بها هذه من المهاجمين عادة،لذا نحتاج إلى إبقائها خارجاً .
- ***صد حركة المرور الصادرة من الشبكة بناءً على المصدر أو الوجهة*** _ بإمكان جدران نار عديدة أن تغربل أيضاً حركة المرور الصادرة من شبكتك الداخلية إلى الانترنت.مثلاً، تريد منع الموظفين من الوصول إلى مواقع الويب الهدامة أو الإباحية .
- ***صد حركة المرور في الشبكة بناءً على المحتوى*** _ بإمكان جدران النار المتقدمة أكثر أن تغربل حركة المرور في الشبكة بحثاً عن محتويً غير مقبول. مثلاً،بإمكان جدار النار المندمج مع مضاد الفيروسات أن يمنع الملفات التي تحتوي على فيروسات من أن تدخل شبكتك. وتندمج بقية جدران النار مع خدمات البريد الإلكتروني لاستبعاد البريد الإلكتروني غير المقبول .
- ***جعل الموارد الداخلية متوفرة*** _ رغم أن الهدف الرئيسي لجدار النار هو منع حركة المرور غير المرغوب بها من عبور الشبكة، يمكنك أيضاً ضبط تكوين العديد من جدران النار للسماح بوصول انتقائي إلى الموارد الداخلية، كخادم ويب عمومي، مع استمرار منع محاولات الوصول الأخرى من الانترنت إلى شبكتك الداخلية.
- ***السماح بالاتصالات إلي الشبكة الداخلية*** _ هناك طريقة شائعة لكي يتصل الموظفون بشبكة وهي استعمال الشبكات الخصوصية الوهمية (الشبكات **VPN**). تتيح الشبكات **VPN** إنشاء اتصالات آمنة من الانترنت إلي شبكة شركة. مثلاً، بإمكان المتصلين عن بعد ومندوبي المبيعات المسافرين أن يستعملوا شبكة **VPN** ليتصلوا بشبكة الشركة. بإمكان الشبكات **VPN** أيضاً أن تربط مكاتب الفروع

ببعضها البعض. يتضمن بعض جدران النار وظائف الشبكة **VPN** ويسهل إنشاء الاتصالات .



VPN اختصاراً للعبارة **Virtual Private Network** "شبكة ظاهرية خاصة" وهي شبكة يتم تأسيسها عبر خطوط هاتف رقمية، ويتم تخصيصها فقط للاتصال بمواقع وحدات تابعة محددة متعددة. يتم استخدام هذه الشبكة لتنفيذ شبكات **WANs** باستخدام الانترنت لإنشاء شبكة شبه خاصة.

- *التبليغ عن حركة المرور في الشبكة وسجلات النار* _ عند غربلة حركة المرور في الشبكة إلى ومن الانترنت، من المهم أيضاً أن تعرف ما الذي يفعله جدار نارك، ومن حاول اقتحام شبكتك، ومن حاول الوصول إلى مواد غير ملائمة على الانترنت، يتضمن معظم جدران النار آلية تبليغ من نوع أو من آخر . بإمكان جدار النار الجيد أيضاً أن يسجل النشاطات في **Syslog** (سجل نظام) أو نوع آخر من وعاء التخزين الأرشيفي. دراسة سجلات جدار النار بعد حصول هجوم هي واحدة من الأدوات الجنائية العديدة التي تتوفر بين يديك.

جدران النار أثناء عملها

من المهم الإشارة إلى أن عدة جدران نار تحتوى واجهتين ماديتين، و**99** بالمئة منها ترتكز على الإيثرنت. تلك الواجهات تسمى الداخل (المحمية) والخارج (غير المحمية) ويتم نشرها بالنسبة لشبكتك. لذا عملياً، تتصل الواجهة الخارجية بالانترنت وتتصل الوجهة الداخلية بشبكتك الداخلية:

١) يفتح المضيف أ، مستعرض ويب ويرغب بمعاينة صفحة ويب. يرسل المضيف أ الطلب عبر جدار النار.

٢) يرى جدار النار الطلب الذي بدأ من المضيف أ والذي يتوجه إلى موقع الويب

أ. يلاحظ جدار النار الطلب الصادر ويتوقع أن الرد سيأتي فقط من خادم

الويب.

ب. توضع علامة جلسة في جدول حالة الجلسات التابع لجدار النار الذي سيتعقب عملية الاتصال من بدايتها إلى نهايتها .

ج. توضع أيضاً قياسات مترية للاتصال في العلامة التي يحافظ عليها جدار النار لهذه المحادثة.

٣) الرد على طلب المضيف أ لرؤية صفحة الويب يُرسل من خادم الويب إلي المضيف أ عبر جدار النار .

٤) يفحص جدار النار جدول حالة جلساته ليرى إن كانت القياسات المترية التي يحتفظ بها لهذه الجلسة تطابق الاتصال الصادر أم لا. إذا كانت كل تفاصيل الاتصال المخزنة تطابق تماماً، يسمح جدار النار بحركة المرور الواردة.

فكر بمسألة واحدة أخيرة تتعلق بجدران النار المبينة للحالة بشكل عام. إذا كان جدار النار يحافظ على سياق حالة الاتصال المتعلقة بالاتصالات الواردة والصادرة، سيصبح من الصعب أن يتمكن قرصان من "تزوير" رزمة بقصد اختراق شبكتك. عندما يحاول المهاجمون إرسال رزم لعبور جدار نار فإن وجود معلومات غير صحيحة عن حالة الاتصال أو عدم وجودها على الإطلاق يعني أن الجلسة ستغلق وعلى الأرجح أنها ستدون لمراجعتها لاحقاً .

أنواع جدران النار

تأتي الكمية الهائلة من جدران النار المتوفرة هذه الأيام في أشكال وأحجام وأصناف عديدة. نوع جدار النار الذي تثبته يعتمد على متطلباتك الدقيقة للحماية والإدارة، وكذلك على حجم شبكتك أو ما الذي سيحميه جدار النار. تقع جدران النار عادة في إحدى الفئات التالية:

جدار النار الشخصي _ جدار النار الشخصي هو عادة برنامج يثبت في كمبيوتر واحد لحماية ذلك الكمبيوتر فقط. هذه الأنواع من جدران النار توضع عادة في الكمبيوترات المنزلية مع الاتصالات العريضة النطاق أو الموظفين البعيدين. بالطبع، كلما أراد شخص نشر جدار نار، يعتبر هذا جيداً.

لقد استجاب صانعو أنظمة التشغيل كشركة أبل ومايكروسوفت لهذه الحاجة وقاموا بدمج جدران نار شخصية فيها. تأتي نظم التشغيل الحديثة مثل **Windows XP/Vista** ومعها جدار نار.

جدار النار المتكامل : هذه الأنواع من جدران النار يستعملها بشكل واسع المشتركون بالاتصال العريض النطاق (الكبل أو **DSL**) الذين يستفيدون من وجود جهاز واحد يقدم الميزات والوظائفية التالية: موجه،بدالة إيثرنت، نقطة وصول لاسلكي، وجدار نار. إذا كان هذا النوع من جدران النار يعجبك، الرجاء التأكد من تحديد قدرات جدار النار بعناية، وكن شكاكاً بالأمان الذي يمكنك اكتسابه من تلك الأجهزة بغض النظر عمن يصنعها .

جدران نار المكاتب الصغيرة إلي المتوسطة : جدران النار هذه، مصممة لتزويد أمان وحماية للمكاتب الصغيرة.

جدران نار الشركات : جدران النار هذه، كسيسكو **PIX 515**، مصممة للمؤسسات الكبيرة التي تضم آلاف المستخدمين، تتضمن ميزات وسعة إضافية، كذاكرة أكثر وواجهات إضافية.

ستشغّل كل جدران نار سيسكو نفس إصدار نظام التشغيل الذي يتضمن نفس قدرات التبليغ والإدارة بغض النظر عن الطراز . ستكون الطُرز الأكبر مطلوبة عندما تكون هناك طلبات لكميات أكبر من الاتصالات والسعة.

عادة يتم تثبيت جدار النار حيث تتصل شبكتك الداخلية بالانترنت. رغم أن المؤسسات الكبيرة تضع أيضاً جدران نار بين مختلف أجزاء شبكتها الداخلية التي تتطلب مستويات مختلفة من الأمان، إلا أن معظم جدران النار تغربل حركة المرور التي تمر عبرها بين الشبكة الداخلية والانترنت. مثلاً، إذا كانت مؤسسة كبيرة تتيح لشركائها المهنيين الاتصال بشبكتها مباشرة، ستجد عادة جدار نار يتحكم بما هو مسموح في شبكة المؤسسة من شركائها. إن وضع جدار نار داخلي بهذه الطريقة يعتبر بالتأكيد شيئاً جيداً .

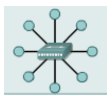
ملخص الفصل

ناقشنا في هذا الفصل واحدة من أهم وأشهر الوسائل لحماية الشبكة وتأمينها. شرحنا ما الذي يجب أن يفعله جدار النار ومن يحتاج إليه ولماذا تحتاج إليه. ناقشنا كذلك كيف يمكن لجدار النار أن يكون أسلوب أمان وكيف يعمل .

أخيراً ناقشنا كيفية تطبيق جدار النار وأنواع جدران النار.

تدريبات

١. هل نحتاج إلي جدار النار ؟
٢. من يحتاج جدار النار؟
٣. لماذا نحتاج إلي جدار النار؟
٤. كيف يكون جدار النار ملحقاً لأسلوب الأمان ؟

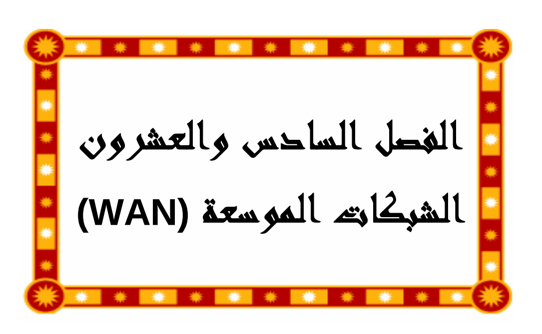


الباب التاسع
التقنيات المتطورة في الشبكات

الفصل السادس والعشرون: الشبكات الموسعة (WAN)

الفصل السابع والعشرون : الشبكات اللاسلكية

الفصل الثامن والعشرون : شبكات VPN



الفصل السادس والعشرون
الشبكات الموسعة (WAN)

*تعرفت في الفصول السابقة علي شبكة **LAN** ومكوناتها وطريقة عملها وكيفية إنشائها ، ولكن ماذا لو زاد عمل الشركة واتسع ليشمل بلداناً وأقطاراً متعددة. ستحتاج بالقطع إلي أكثر من شبكة **LAN** مرتبطة ببعضها بوسيلة ما. من هنا جاءت فكرة شبكة **WAN**. فهي شبكة مكونة من شبكتي **LAN** أو أكثر متصلين بواسطة خطوط هاتف رقمية ويتم توجيهها بين مقاطع.*

بانتهاء هذا الفصل ستتعرف علي :

- *ما هي شبكة **WAN** ومن يحتاج إليها.*
- *مكونات شبكة **WAN**.*
- *الموجهات.*
- *بروتوكولات الموجه.*
- *خطوط نقل البيانات.*
- *خطوط **DSL**.*
- *الانترنت وشبكة **WAN**.*

نشأت فكرة شبكة **WAN** أو شبكة الاتصال الواسعة من الحاجة إلى القدرة على نقل البيانات عبر مسافات طويلة بسرعة كبيرة لقد كانت الشبكات الأولى بطيئة ومحدودة المدى. لكن مع التطور الذى أصاب الحياة بصفة عامة وتكنولوجيا الاتصالات بصفة خاصة، ابتكرت شركات ربط الشركات طرق لربط الشبكات معاً تسمح للمستخدمين بالاتصال من مسافات طويلة إلى نفس البيانات ولكن ما هى شبكة **WAN**؟

ما هي شبكة WAN (Wide Area Network)

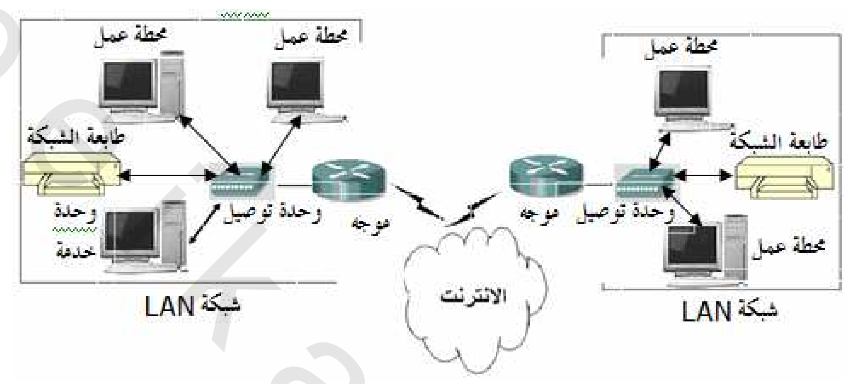
عبارة عن مجموعة شبكات محلية متعددة **(LANs)** توجد عادة فى مواقع مختلفة يتم وصلها ببعضها البعض.

إذن تسمية شبكة واسعة أو موسعة **(WAN)** جاءت من طبيعة عملها حيث تربط شبكتى كمبيوتر محلية أو أكثر موجودة فى مواقع جغرافية متفرقة معا. يتم ربط شبكات **WAN** باستخدام خطوط هاتف عالية السرعة. يتشارك مستخدمو الكمبيوتر على شبكة **LANs** متعددة فى الموارد. ولكن فى الحقيقة هذا التعريف تبسيط لحقيقة شبكة **WAN** وطبيعة عملها، يتضح ذلك من المثال التالى:

عندما تستخدم بطاقة الائتمان الخاصة بك **Credit Card** فى أحد المحلات لدفع قيمة مشترياتك أو لسداد فاتورة خدمة معينة. يتم الحصول على هذه الخدمة عن طريق شبكة **WAN**. لأن الذى يحدث بالضبط أن الجهاز الذى يستخدمه الصراف رغم أنه لايعد جهاز كمبيوتر بالمعنى المعروف وإنما هو جهاز ذو أغراض محدودة جدا. يقوم هذا الجهاز بالبحث فى قواعد بيانات الشركات المشتركة فى الخدمة عبر خطوط هاتف مؤجرة للتأكد من بطاقة الائتمان وصلاحيتها.

من هذا المثال نفهم أن شبكة **WAN** تعتبر طريقة لمد موارد الشبكة فيما وراء المنطقة المحلية. وفى عصر الإنترنت، توجد الكثير من الطرق لتنفيذ ذلك منها مثلا خطوط الهاتف الرقمية باهظة التكاليف ونوع من الشبكات يسمى **Virtual Private Network** (شبكات ظاهرية خاصة) تختصر هكذا **VPN**. (وهى طريقة لتوصيل الشبكات تستخدم الإنترنت لحمل الشبكات) .

يوضح شكل ١-٢٦ فكرة شبكة **WAN** في هذا الشكل تم ربط شبكتي **LAN** تتكون كل منهما من وحدة خدمة **Server** ووحدتين تابعتين وتستخدم وحدة توصيل **Hub** لربط الوحدات التابعة وتربط الموجهات (**Routers**) بين الشبكات لتكون في النهاية شبكة **WAN**.



شكل ٢٦-١ ربط شبكتي **LAN**

تستخدم شبكات **WAN** أنواع من الروابط للربط بين الشبكات المحلية **LAN** منها

- موجات الميكروويف **Microwave**.
- الأقمار الصناعية **Satellites**.
- أسلاك الألياف البصرية **Fiber Optic**
- الأسلاك المحورية **Coaxial cables**

من يحتاج إلى شبكة WAN

حيث أن شبكة **WAN** تمتد إلى مناطق جغرافية متفرقة وتستخدم تقنيات باهظة التكاليف كما أوضحنا قبل قليل، فإنها تعد بواسطة الشركات الكبرى أو المؤسسات التى ترغب فى تأسيس وجود شبكى مهم فى أنحاء القطر الواحد أو حتى فى أنحاء العالم.

ورغم أن هذه الشبكة باهظة التكاليف، إلا أن الفائدة التى تجنيها الشركات الكبرى من ورائها يمكن أن تتفوق على التكاليف عدة مرات.

تصور مثلا شركات الطيران التى تحتاج لإدارة بيانات الرحلات الجوية فى المطارات بدون شبكة **WAN** بالطبع لن تستطيع تقديم أى نوع من الخدمات لعملائها.

مكونات شبكة WAN

أجهزة المودم Modems

كلمة **Modem** اختصار لعبارة **Modulator / demodulator** ومعناها "تعديل – إلغاء التعديل). ويستخدم أساسا لتبادل البيانات بين أجهزة الكمبيوتر عبر خطوط الهاتف وهو جهاز يستخدم لتحويل إشارات الكمبيوتر الرقمية **(Digital)** إلى إشارات قياسية **(Analog)** ثم تنتقل تلك الإشارات القياسية من خلال خطوط التليفون عند الإرسال. وعند الاستقبال (فى الجهاز المستقبل) يقوم المودم بعملية عكسية أى يتم تحويل الإشارات القياسية إلى إشارات رقمية يفهمها الكمبيوتر.

تقاس سرعة المودم فى نقل البيانات بعدد البتات **(Bits)** فى الثانية وتختلف تلك السرعات باختلاف نوع المودم وسعره. وهى تتراوح بين **٢٤٠٠** إلى **٥٧٠٠** بايت فى الثانية (**٥٦** كيلوبايت).

يوجد نوعين من أجهزة المودم : مودم داخلي : وهو عبارة عن بطاقة تركب داخل جهاز الكمبيوتر فى إحدى فتحات التوسعة **Expansion Slots** الموجودة على اللوحة الأم لجهاز الكمبيوتر، مودم خارجى: ويكون منفصلا عن جهاز الكمبيوتر ويتصل به بواسطة سلك توصيل يستخدم المودم نوعين من خطوط الهاتف.

*خطوط الهاتف العادية **Dial-up network Lines**:*

وفى هذا النوع يقوم المستخدم بإجراء اتصال تليفونى فى كل مرة يرغب فيها فى استخدام المودم

*الخطوط المؤجرة **Leased lines***

وهى خطوط تعمل على مدار **٢٤** ساعة ولا تحتاج إلى إجراء اتصال تليفونى وهى أسرع وأجود من خطوط الهاتف العادية.

الجسور Bridges

الجسر **Bridge** عبارة عن جهاز يستخدم للربط بين الشبكات المحلية **LAN** وتوسيعها. ويمكنه التوصيل بين شبكات ذات تصميمات مختلفة مثل شبكات **Ethernet** مع شبكات

كما يمكنه الربط بين شبكات تعمل باستخدام بروتوكولات مختلفة مثل **Token Ring** و **IPX** و **TCP**.

تعد الجسور أجهزة قديمة لم تعد مستخدمة كثيراً، ولكننا أوردناها هنا لأنك قد تصادفها في المواقع القديمة، لايعد استخدام الجسور لربط الشبكات طريقة فعالة لمعالجة اتصالات **WAN**. نظراً لأن الجسر يمرر تدفق اتصالات البث (وهي الرسائل التي يتم إرسالها إلي كل جهاز علي شبكة معينة) وهذا يهدر بعض تردد نطاق ارتباط **WAN** .

بصفة عامة يعد الجسر (**Bridge**) موجهاً تم توصيفه لتوصيل الشبكات عند طبقة **Data Link** "ربط البيانات" وهي الطبقة رقم ٢ من نموذج **OSI** بدلاً من طبقة **Network** "شبكة الاتصال" من النموذج. وهي الطبقة التي تعمل فيها الموجهات (**Routers**). عندما يربط جسر الشبكات، يتم توسيع الشبكة الحالية بحيث يري المستخدمون إصداراً أكبر من الشبكة المحلية، ويمكنهم الوصول إلي الموارد البعيدة بنفس الطرق المستخدمة في شبكة **LAN**. ولأن الجسور تعتبر بطيئة، فيتم استخدام الموجه (**Router**) لربط شبكات **LAN** في الوقت الحالي بدلاً من الجسور (**Bridges**). وبالتالي لم يعد استخدام الجسر مستخدماً. سوف نشرح بعد قليل الموجهات، وستعرف الفرق بينها وبين الجسور.

تتعرف الجسور على أجهزة الكمبيوتر على الشبكة بأن ترسل رسائل موجهة إلى كل الأجهزة، وعندما تقوم الأجهزة بالرد تتعرف الجسور على عناوين تلك الأجهزة ومواقعها. ثم تستخدم تلك المعلومات لإنشاء جدول توجيه **Routing Table** وهناك طريقة أخرى تستخدمها الجسور للتعرف على الأجهزة وهى الكشف عن حزم البيانات المارة بها، ويقوم الجسر بمقارنة عنوان الكمبيوتر المرسل للحزمة مع العناوين المخزنة فى جدول التوجيه (**Routing Table**). وفى حالة عدم عثور الجسر على العنوان يقوم بإضافته إلى الجدول. وهكذا يتم تحديث الجداول بصفة مستمرة.

مترجمات البروتوكولات Protocol Translators

عبارة عن أجهزة يمكنها الترجمة بين بروتوكولين من بروتوكولات الشبكة. تستخدم مترجمات البروتوكولات لترجمة بين بروتوكول **IPX** لشبكة **NetWare** وبروتوكول

TCP/IP حتى يمكن للشبكات التى تعتمد على IPX الاتصال بالإنترنت إذا كنت تستخدم شبكة NetWare، قد يكون بروتوكول الترجمة أفضل طريقة لتمكين وصول الإنترنت للمستخدمين.

على الرغم من ذلك ، يعد بروتوكول IPX NetWare الأساس وهو قابلا للتوجيه، وربما يكون الموجه (Router) اختياراً أفضل إذا كنت ترغب فى ربط شبكتى LANs لإنشاء شبكة WAN، تابع قراءة البند التالى للتعرف على الموجهات

الموجهات Routers

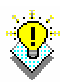
يمكن تعريف الموجه (Router) بأنه جهاز يقوم بمعالجة وتمرير حزم البيانات داخل الشبكة الواحدة أو بين شبكات LAN منفصلة ويتم إرسال البيانات من مصادرها إلى وجهاتها فى أسرع طريق ممكن.

يعمل الموجه عند طبقة NetWare (شبكة الاتصال) **وهى الطبقة الثالثة فى نموذج OSI الذى مر بنا .**

فى حالة الشبكة الواحدة، تتجه حزم البيانات من الجهاز المرسل إلى الجهاز الوجهة دون أية وسائط. أما إذا كان عنوان الوجهة لحزمة البيانات خارج الشبكة المحلية، سيتم إرسالها إلى الموجة (الذى يعرفه الجهاز المرسل بصفته المدخل الافتراضى) **بدون معالجتها.**

عندما يتلقى الموجه حزمة بيانات موجهة لمكان خارج الشبكة المحلية، سوف يقوم الموجه بإرسال حزمة البيانات إلى النقطة التالية.

وللتوضيح نقول . ترسل الموجهات حزم البيانات وفقا للموجهات المتوفرة بين الشبكات وتحاول تحديد أقصر مسار توجيه ممكن فى أى وقت محدد. كيف يتم ذلك؟ يوجد داخل الموجه (وهو جهاز كمبيوتر صغير لكنه قوى جدا) **توجد مجموعة بيانات تسمى Routing Tables أو "جداول التوجيه". يتم تحديث هذه الجداول بواسطة بروتوكولات توجيه يطلق على أحدها Routing Information Protocol (RIP) أو "برتوكول توجيه المعلومات" وعلى الثانى Open Shortest Path first (OSPF) "فتح أقصر مسار أولا".**



سنتعرض لشرح كلا من RIP وOSPF فى البند التالى

ويقوم أى من البروتوكولين بتمرير البيانات بصفة مستمرة بين الموجهات للتأكد أن كل الموجهات لديها أحدث البيانات فيما يتعلق بمسارات التوجه المتوفرة.

كيف يتم توجيه البيانات

تحتوى جداول التوجيه على جميع مسارات التوجيه الممكنة، ويستعين الموجه بجداول التوجيه لتحديد ما إذا كان لديه مسار توجيه إلى عنوان وجهة معين أو لا.

إذن كل ما يفعله الموجه هو إعادة إرسال حزم البيانات إلى وجهاتها. ويحاول الموجه فعل ذلك بأفضل طريقة كيف ذلك ؟ فى كل مرة يتم توجيه حزمة البيانات بين موجه وآخر يزيد رقم فى حزمة البيانات يطلق عليه عدد الوثبات أو العداد بمقدار واحد (١) إذا وصل عدد الوثبات إلى عدد من المرات محددة سلفا (مثلا يسمح لبروتوكول RIP بعدد ١٦ وثبة بين المصدر والوجهة) يتم تجاهل حزمة البيانات، باعتبار أن الموجه حاول ١٦ مرة ولم يفلح فى تسليمها إلى عنوان الوجهة.

بروتوكولات الموجه Router Protocol

تستخدم الموجهات مجموعة من البروتوكولات لتحديد الطريقة المناسبة لتوجيه حزم البيانات. تسمى هذه البروتوكولات "بروتوكولات المداخل" أو **Gateways Protocols**. وتعد هذه البروتوكولات أفراداً فى مجموعة بروتوكولات **TCP/IP** التى تستخدمها الموجهات لتحديد أفضل مسار توجيه لحزم البيانات.

شرحنا في الفصل الثامن عشر بالتفصيل بروتوكولات الموجه وهي تستخدم أساساً في الشبكات الواسعة لذلك. لا نري ضرورة لإعادة تكرار الشرح هنا، ننصح بالرجوع إلي الشرح السابق عن بروتوكولات التوجيه في الفصل الثامن عشر للتعرف علي البروتوكولات المستخدمة في التوجيه بالتفصيل.

خطوط نقل البيانات

عادة يتم ربط شبكات **WANs** باستخدام خطوط هاتف رقمية **Digital Phone Lines**. توفر خطوط الهاتف الرقمية سرعات عالية جدا لنقل البيانات عبر مسافات بعيدة، تقوم خطوط الهاتف الرقمية بتحويل الصوت العادى إلى بيانات رقمية **Digital Data**والبيانات الرقمية هى البيانات التى يفهمها الكمبيوتر والتى تتكون من الصفر والواحد والتى تعرف بالنظام الثنائى.

ولتوضيح الفرق بين خطوط الهاتف الرقمية وخطوط الهاتف القياسية نجد أن خطوط الهاتف القياسية **Analog Phone Lines** مثل تلك التى تستخدمها فى مكتبك للاتصال بعملائك ترسل الصوت على شكل موجات (مثل موجات الراديو).

لإرسال البيانات من التليفون القياسى (التليفون المتصل ببيتك أو مكتبك) يجب تحويلها من الصوت إلى بيانات رقمية. ويستخدم لهذا الغرض عادة جهاز المودم **Modem** وفيما يلى نوضح أشهر الخطوط الرقمية المستخدمة فى نقل البيانات.

خطوط T1 و T3 الرقمية

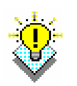
تعرف خطوط **T1** و **T3** بالخطوط الرئيسية. وهى خطوط رقمية تماما وتغطى هذه الخطوط نطاقا واسعا من احتياجات ربط الشبكات ويعتبر نظام الخطوط الرئيسية هو أول نظام خطوط هاتف رقمية. يوفر خط **T1** معدل إرسال يصل إلى **1.544** ميجابت فى الثانية، ويتم استخدامه غالبا لتوصيل شبكات **WANs** داخليا، بينما تبلغ سرعة خط **T3** **44.736** ميجابت فى الثانية، ويستخدم عادة بواسطة الشبكات الكبيرة ومزودى خدمة الإنترنت، لأن تكلفة هذا الخط عالية جداً ولا تقدر عليها الشركات الصغيرة.

قد لا توجد خطوط **T3** إلا إذا كنت تعمل لصالح مزود خدمة انترنت أو كان لديك اتصال بمركز بيانات رئيسى. حيث تصل سرعتها إلى حوالى ٤٥ ميجابت فى الثانية. بالنسبة لشبكات **WANs** الصغيرة والمتوسطة يكفى استخدام خط **T1**. بل قد تستخدمه جزئيا لعدم حاجتك إلى استخدامه كاملاً .

الخطوط المؤجرة Leased Lines

كثيرا ما يطلق على الخطوط الرئيسية **Leased Lines** (الخطوط المؤجرة). وتستخدم عادة بواسطة شركة أو مؤسسة واحدة.

تمر الخطوط المؤجرة بين نقطتين . ويمكن أن تكون هاتين النقطتين فرعين لشركتك أو قد تكون واحدة منهما شركتك والأخرى موقع لمزود خدمة انترنت يزودك بخدمات الإنترنت.



توفر شركات الاتصالات الكثير من الطرق لحساب رسوم خطوط الهاتف الرقمية. وتختلف تلك الرسوم من شركة لأخرى.

نقل البيانات عبر الخطوط الرقمية

يتم نقل البيانات عبر خطوط الهاتف الرقمية باستخدام طريقتين الأولى تسمى **frame relay** (نقل الأطر) والثانية **Clear channel signaling** وتختصر عادة **CCS** وتعنى "إشارة القناة الواضحة".

يتم استخدام نقل الأطر **Frame relay** فى الغالب للاتصال بالإنترنت بالإضافة إلى استخدامه لربط مواقع متعددة. من السهل استخدام نقل الأطر ولكنه أقل كفاءة من **CCS** "خط قناة واضح".

أحيانا يطلق على طريقة **Clear channel signaling** "إشارة القناة الواضحة" اسم **Common channel signaling** "إشارة القناة العامة" وهما بنفس المعنى، وهى طريقة لتعويض عدم كفاءة طريقة **Frame Relay** لنقل البيانات.

فى طريقة **CCS** يتم إرسال كل الإرشادات عن كيفية نقل البيانات عبر قناة منفصلة عن البيانات ولذلك ليست هناك حاجة لوضع البيانات فى أطر البيانات الخاصة بها. وبالتالى سوف تحصل على مخرجات أعلى.

فى المقابل فإن تكلفة طريقة **CCS** (طريقة القناة الواضحة) أعلى بكثير من طريقة نقل الأطر.

الخطوط المشتركة الرقمية DSL

الطريقة الأرخص والأوفر لنقل البيانات باستخدام خطوط الهاتف الرقمية هى **Digital Subscriber Line** وتختصر هكذا **DSL** وتعنى "خط المشترك الرقمى" توفر هذه الخطوط خدمة ممتازة للاتصال بالإنترنت. أصبحت خدمة **DSL** منخفضة يمكن أن يتحملها المشترك. كما أنها سهلة التزويد من قبل شركات الاتصالات. وقد انتشرت خدمة **DSL** وأصبح من الممكن الحصول عليها من قبل مزودى خدمة الإنترنت وليس شركات الاتصالات فقط.

من مزايا **DSL** أن تكلفتها أقل بكثير من تلك الخاصة بخدمة خط **T1** والثانية أنها تمر عبر نفس السلك النحاسى التى تستخدمه خطوط الهاتف العادية، والثالثة أنها توفر سرعة عالية جدا لنقل البيانات.

وعلي الرغم من فوائد **DSL** فإن لها بعض العيوب. ففي معظم الحالات تعد أقصي مسافة لدوائر **DSL** الكهربائية أقل من ستة أميال فإذا كانت المسافة بين مكتبك والمكتب الرئيسي للشركة أكثر من تسعة أميال لن تتمكن من استخدام الخدمة. يمثل ذلك مشكلة محتملة بالنسبة لإضافة **DSL** إلي شبكات **WANs** الموجودة في الأقاليم.

تتوفر **DSL** فى مجموعة مختلفة من التوصيفات أشهرها:

- **ADSL** : كلمة **ADSL** اختصار لعبارة **Asymmetric Digital Subscriber Line** ومعناها "خط مشترك رقمى غير متماثل" وتعد **ADSL** مفيدة جدا للوصول إلى الإنترنت لأن البيانات التى تأتى للشبكة تعد أهم من البيانات التى تخرج منها. في حين لا تعد مفيدة بالنسبة لشبكات **WAN** .

  يستخدم الكثيرين ممن يستخدمون **DSL** فى المنازل هذا التوصيف من **DSL**. لأن المستخدمين في المنازل يُحمِّلون قدراً أكبر بكثير من الانترنت إلي أجهزتهم المنزلية مما يحملونه إلي أعلي (يرسلونه عبر الانترنت).

- **HDSL**: كلمة **HDSL** اختصار للعبارة **High-speed Digital Subscriber Line** أو "خطوط المشترك الرقمى عالية السرعة".

ويعتبر هذا الشكل من DSL أكثر فائدة لشبكات WANs ، حيث ترسل HDSL البيانات بسرعات تصل إلى معدلات خط T1(1.544 ميجابايت فى الثانية) وتصل إلى مسافات طويلة.

الانترنت وشبكة WAN

مع وضع التكاليف المرتفعة لخدمة الهاتف الرقمية في الاعتبار، يمكن أن يصبح إنشاء شبكة بها الكثير من المواقع البعيدة المرتبطة بخطوط رقمية أمراً باهظ التكلفة بسرعة كبيرة. يعد جزء من هذه التكلفة لا مفر منه؛ لتوصيل الشبكات معاً على أساس مستمر يمكن الاعتماد عليه، تعد خدمة الهاتف الرقمية ضرورية. على الرغم من ذلك، هناك تكاليف تزايدية إضافية لتطوير شبكة WAN خاصة، مثل: تكلفة رواتب مدير نظام واحد أو أكثر والنفقات الإضافية التي تأتي مع إدارة شبكة خاصة.

تتمثل إحدى الطرق لتقليل تكاليف إدارة WAN في تكليف جهة أخرى بإدارتها، أو توظيف شخص آخر للتعامل مع ربط شبكة LAN الداخلية من أجلك.

على الرغم من ذلك، مع زيادة حجم الإنترنت، دخل الكثير من كبار مزودي خدمة الإنترنت في مجال توفير خدمات WAN. وعرض هؤلاء خدمات الاتصال بصفتها الخدمة التي يتم بيعها. لقد اختار مزودو خدمة الإنترنت تحمل جزء كبير من تكلفة دمج خطوط الهاتف الرقمية وتكنولوجيا WAN، واختاروا بدلاً من ذلك تحقيق الربح من خدمة الشبكة التي يتم تزويدها.

على أيه حال، لنموذج مزود خدمة الإنترنت جانب إيجابي آخر: يعد مزودي خدمة الإنترنت مجرد شبكات توجيه تعتمد على أجهزة الكمبيوتر. نظراً لأن مزود خدمة الإنترنت لديه شبكة تعتمد على أجهزة الكمبيوتر، فمن المؤكد أنه سوف يعد شبكات WANs مؤمنة نسبياً، ويمكن الاعتماد عليها من أجل العملاء.كيف يفعلون ذلك؟ يتوفر لمزودي خدمة الإنترنت خبرات ربط الشبكات بالفعل، والأهم من ذلك، أنهم لديهم البنيات الأساسية لربط الشبكات. يتم تصميم البنية الأساسية لربط الشبكات الخاصة بمزود خدمة الإنترنت بغرض تحديد قدر البيانات التي تتجه من النقطة (أ) إلى النقطة (ب)

وتعود مرة أخرى. إذا أعد مزود خدمة الإنترنت الموجهات لتوجيه حزم بيانات تأتي من شبكات معينة إلى شبكات أخرى معينة فقط وتستخدم الإنترنت بصفتها وسيلة نقل بين مواقع خدمة مزود خدمة الإنترنت، يعني ذلك أنه أعد نوعاً من شبكة **WAN** يطلق عليه **Virtual Privet Network (VPN)** (شبكة ظاهرية خاصة). لكل الأغراض العلمية، تنفذ **VPN** نفس المهام التي تؤديها شبكة **WAN** مخصصة تعتمد على خط هاتف رقمي من نقطة إلي نقطة، ولكن بصفة عامة، تتكلف هذه الشبكة أقل وتتطلب صيانة أقل من المستخدم النهائي. مادام مزود خدمة الإنترنت يؤدي مهمته، يجب تضمين تكاليف صيانة ارتباطات الشبكة الداخلية ضمن الرسوم الشهرية لمزود خدمة الإنترنت. هناك بعض المحاذير المهمة بشأن **VPN**. أولاً: تستخدم الإنترنت لتوجيه بعض بياناتها أو كلها. من الواضح أن الإنترنت كما توجد حالياً لا تعد مكاناً مؤمناً بصورة تامة. هناك طرق لالتقاط الكثير من تدفق اتصالات الشبكة، إذا عرف شخص ما كيفيه ذلك. إذا التقط هذا الشخص تدفق اتصالات يحتوي على معلومات بطاقة ائتمان غير مشفرة أو مذكرات سرية، يمكن أن تقع في مشكلة كبيرة. إذا قررت أن استخدام **VPN** يبدو فكرةً جيدةً، تعلم أولاً كيفية تأمين أجهزة الكمبيوتر (كما مر بنا في الباب الثامن) ونفذ الأمر بصورة صحيحة. تعد شبكات **VPNs** حلاً جيداً للمعركة القديمة بين التكلفة والميزات، ولكن فقط إذا تم إنشاؤها بصورة صحيحة. إذا فعلت ذلك بطريقة صحيحة، يمكنك زيادة قوة الإنترنت لتلبية احتياجاتك .

ملخص الفصل

شرحت في هذا الفصل فكرة شبكة **WAN** والفرق بينها وبين شبكة **LAN** ومن يحتاج إليها. شرحنا بعد ذلك الأجهزة المستخدمة مع شبكات **LAN**، مع التركيز علي الموجهات **Routers**. شرحنا أيضاً الخطوط الرقمية المستخدمة في نقل البيانات مثل خطوط **T1** و **T3** الرقمية لأن شبكات **WAN** هي التي تحتاج لهذه الخطوط السريعة لتباعد المسافات التي تغطيها. أخيراً قدمنا فكرة عن شبكات **VPN** باعتبارها بديلاً رخيصاً لشبكة **WAN**. ووسيلة لزيادة قوة الانترنت لتلبية احتياجاتك.

تدريبات

١. متي يقال عن شبكة ما أنها شبكة WAN ؟

٢. ما نوع خطوط الهاتف التي يمكن أن تستخدمها شبكة WAN ؟

٣. ضع علامة (✓) أمام العبارة الصحيحة وعلامة (✗) أمام العبارة الخطأ.

أ. من مزايا شبكة WAN أنها قليلة التكاليف.

ب. شبكة WAN عبارة عن مجموعة شبكات LAN مرتبطة ببعضها.

ج. الموجهات جزء أساسي في شبكات WAN. ولا يمكن الاستغناء عنها في هذا النوع من الشبكات.





يناقش هذا الفصل استعمال شبكات LAN اللاسلكية والتي تسمي WLAN (Wireless LAN) والتي يزدهر استعمالها في كل مكان تقريباً. في المطاعم والمقاهي والمطارات والفنادق وحتي منازل الأشخاص.

بالانتهاء من هذا الفصل ستتعرف علي :

- ***ما هي الشبكات اللاسلكية***
- ***معيار 802.11***
- ***كيف تنشئ شبكة تجمع بين مكونات سلكية ولاسلكية***
- ***وصل الشبكات اللاسلكية***
- ***كيفية استخدام شبكة لاسلكية***
- ***المخاطر الأمنية التى تتعرض لها الشبكات اللاسلكية***
- ***كيف نحمي الشبكة اللاسلكية***

تقنية الشبكة اللاسلكية

تعتمد شبكة LAN والشبكات الموسعة WAN على الأسلاك وتعتبر الأسلاك فى الشبكات السلكية طريقة فعالة لنقل البيانات.

مرت الكابلات (الأسلاك) بتطورات متعددة شأنها شأن بقية مكونات الشبكة – أصبحت خلالها أصغر وأسهل استخداما

كانت الأسلاك سميكة وثقيلة الوزن وكان يصعب طيها. ثم ظهر كابل Coax الذى أصبح أخف وزنا وأسهل استخداما. ثم ظهر كابل UTP (Unshielded Twisted Pair) ليصبح هو الكابل القياسى. ولذلك فمعظم الشبكات تستخدمه فى هذه الأيام

ولكن نظرا للمشاكل التى تواجه الأسلاك كوسط إرسال حيث أن جميع الكابلات تتطلب إحداث ثقوب فى الحوائط وسحبها من خلالها وعبر الأسقف لإنشاء شبكة تغطى شركتك أو مصنعك نتيجة لهذه المشاكل نشأت فكرة استخدام الشبكات اللاسلكية.

لقد أدي نمو أجهزة الكمبيوتر في الثمانينيات إلي إنشاء شبكات LAN، أو إنشاء شبكة الانترنت في التسعينات، مما وفر إجراء اتصالات بغض النظر عن المكان الجغرافي. برهنت الشبكات WLAN علي أنها منطقة النمو التقنية بدءاً من القرن الحادي والعشرين .

تعتبر الشبكات المحلية اللاسلكية WLAN (Wireless LAN) حاليا من الخيارات الفعالة فى مجال الشبكات. ويرجع ذلك إلي التطور الكبير فى التقنيات اللاسلكية وانخفاض أسعار منتجاتها.

تظهر أهمية تقنية الشبكات اللاسلكية عندما ترغب فى ربط أجهزة الكمبيوتر محمولة بالشبكة، حيث يمكنك حيث يمكنك حمل الجهاز واستخدامه من أى مكان.

الشبكة اللاسلكية

الشبكة اللاسلكية عبارة عن شبكة تعتمد على موجات الراديو لتبادل المعلومات بدلا من الكابلات التقليدية. تشبه الشبكة اللاسلكية شبكة الهاتف المحمول (الجوال) من حيث أن المستخدم يمكنه التنقل بحرية من مكان لآخر ويظل متصلا بالشبكة من خلال جهاز

الكمبيوتر المحمول الخاص به دون أن يتصل بكابل الشبكة.

تقدم الشبكات **WLAN** ملحقاً سريعاً وفعالاً لشبكة **LAN** سلكية. بمجرد تثبيت نقاط وصول إلي الشبكة اللاسلكية تصبح أجهزة الكمبيوتر المكتبية والمحمولة المجهزة ببطاقات **LAN** لاسلكية قادرة علي الاتصال بالشبكة السلكية بسرعات عريضة النطاق (أو أكبر) بمسافة تصل إلي ٢٧٥ متراً عن نقطة الوصول اللاسلكي. هذا يعني أن أجهزة الكمبيوتر لم تعد مربوطة بالبنية التحتية للأسلاك. حرية تامة.... أليس كذلك ؟؟؟

من مزايا الشبكة اللاسلكية رغم المصاعب التى ترد عليها والتى سيرد ذكرها فى نهاية هذا الفصل ما يلى:

- عملية بالنسبة للأشخاص كثيرى التنقل.
- مناسبة للأماكن التى يصعب استخدام الأسلاك فيها.
- توفير الاتصالات فى الأماكن المزدحمة.

يحتوى كل جهاز كمبيوتر فى الشبكة اللاسلكية على جهاز مرسل مستقبل **Transceiver** لاسلكى يقوم باستقبال الإشارات وإرسالها إلي أجهزة الكمبيوتر المحيطة.

من الأجهزة التى تستخدم الشبكة اللاسلكية أجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر الشخصية والتليفونات الجوالة. يطلق على الشبكات اللاسلكية عبارة **Wireless Local Area Network** وتختصر هكذا **WLAN** كما يستخدم مصطلح **Wi-Fi** عادة للإشارة إلي الشبكات اللاسلكية رغم أنه من الناحية الفنية يشير إلي نوع واحد فقط من هذه الشبكات هو تلك التى تعتمد على معيار **802.11b** (سنشرح المعيار **802.11b** بعد قليل)

تستخدم الشبكات اللاسلكية ما يعرف بـــ **Service Set identifier** وتختصر هكذا **SSID**. ومعناها "معرِّف محدد الخدمة لتعريف الشبكة اللاسلكية. وتعرف الشبكات اللاسلكية باسم **SSID**. وعادة تستخدم جميع أجهزة الكمبيوتر المتصلة بنفس الشبكة اللاسلكية نفس **SSID**.

تستخدم الشبكات اللاسلكية جهاز يسمى **(WAP) Wireless Access Point** لوصل أجهزة الكمبيوتر اللاسلكية بالشبكة السلكية الموجودة بالفعل.

معيار 802.11

أكثرية الشبكات WLAN قيد الاستخدام تستعمل معياراً قياسياً للإرسال اللاسلكي معروف كـ 802.11B. يعمل المعيار القياسي IEEE 802.11B عند تواتر الراديو 2.4 جيجاهرتز – وهو تواتر غير منظم من قبل الحكومات. يقدم المعيار القياسي 802.11b سرعات اتصال تصل إلي 11 ميجابت في الثانية ، وهذه سرعة كافية لمعالجة مرفقات البريد الإلكتروني الكبيرة ولتشغيل البرامج المرهقة لعرض نطاق البث كمؤتمرات الفيديو. بينما أصبح المعيار القياسي 802.11b يهيمن الآن على سوق الشبكة LAN اللاسلكية، يتم تطوير تنويعات أخرى عن المعيار القياسي 802.11، أو تمت الموافقة عليها من قبل، لمعالجة السرعات المتزايدة. 802.11g هو أحداث إصدار عن المعيار، وهو يقدم سرعات لاسلكية تصل إلي 56 ميجابت في الثانية.

إن مختلف المعايير القياسية اللاسلكية تستهدف مجالات مختلفة في الصناعة كما هو مبين في الجدولين ٢٧–١ و ٢٧–٢ .

الجدول ٢٧–١ المميزات القياسية لـــ 802.11a/ WLAN

المعيار القياسي	WLAN , IEEE 802.11a
الطول الموجي للتواتر	5 جيجاهرتز
عرض نطاق بث البيانات	54 ميجابت بالثانية،48 ميجابت بالثانية، 36 ميجابت بالثانية، 24 ميجابت بالثانية، 12 ميجابت بالثانية،6 ميجابت بالثانية
نطاق التشغيل الأمثل	45 متر في البيت، 90 متر في الهواء الطلق
الأفضل لهدف معين أو نوع أجهزة	الكمبيوترات المحمولة المتجولة في المنزل أو الشركة؛ الكمبيوترات المكتبية عند تمديد الأسلاك غير مريحة

الجدول ٢٧-٢ المميزات القياسية لـــ 802.11g / Wi-Fi

المعيار القياسي	Wi-Fi , IEEE 802.11g
الطول الموجي للتواتر	2.4 جيجا هيرتز
عرض نطاق بث البيانات	54 ميجابت بالثانية، 48 ميجابت بالثانية، 36 ميجابت بالثانية، 24 ميجابت بالثانية، 12 ميجابت بالثانية، 6 ميجابت بالثانية
نطاق التشغيل الأمثل	300 متر في الظروف المثالية؛ توقع مسافة أشبه ب 45 متر في البيت و 90 متر في الهواء الطلق في الظروف العادية
الأفضل لهدف معين أو نوع أجهزة	الكمبيوترات المحمولة المتجولة في المنزل أو الشركة؛ الكمبيوترات المكتبية عند تمديد الأسلاك غير مريحة

لم يحقق 802.11a أى نجاح أبداً، لكن المعيار 802.11g المقر مؤخراً يتضمن بعض الخيارات المثيرة للاهتمام ليشمل المزيد من السرعة والأمان مثلما يبين الجدول ٢٧-٢.

لاحظ أنه عندما يُمنح عملاء 802.11b وصولاً إلي نقطة وصول لاسلكي 802.11g، لا مفر من ضبط (تخفيض) الأمان للسماح لعملاء 802.11b، بالدخول ؛ بفضل WEP ومشاكلها، تنخفض الشبكة بأكملها إلي أدنى مقام كسر شائع.

ما هو Wi-Fi ؟

يستعمل المصطلح Wi-Fi (اختصار Wireless Fidelity ، "الدقة اللاسلكية") في أغلب الأحيان في مناقشات الشبكات Wi-Fi.802.11 أو هي بالتأكيد الكلمة التسويقية الشعبية المستعملة هذه الأيام عند التكلم عن اللاسلكي. لقد بدأ المصطلح Wi-Fi بسرعة يصبح الطريقة الشائعة لوصف الشبكات 802.11 اللاسلكية.

يشير Wi-Fi أيضاً إلي شهادة من Wi-Fi Alliance، وهي اتحاد دولي لا يبغي الربح، يتألف من باعة المنتجات 802.11. إن منتجات 802.11 التى تنال الشهادة

Wi-Fi قد تم اختبارها ووجدت أنها قابلة للعمل بشكل متبادل مع المنتجات الأخرى المصادق عليها. هذا يعني أنه يمكنك استعمال منتجك الذي يحمل الشهادة Wi-Fi مع الشبكات 802.11 التي تحمل الشهادة Wi-Fi، سواء كانت كمبيوترات أبل أو شبكات مؤسسة على Windows. رغم أن منتجات 802.11 التي لا تحمل الشهادة Wi-Fi قد تعمل جيداً مع الأجهزة التي تحمل تلك الشهادة، إلا أن الشعار Wi-Fi Certified هو ضمانتك لقابلية العمل المتبادل. يمكنك أن تتعلم أكثر عن Wi-Fi Alliance على الانترنت في /http:// www. Weca.net .

فوائد الشبكات اللاسلكية

- **سعر جذاب – نشر شبكة LAN لاسلكية يمكن أن يكون أرخص من شبكة LAN سلكية لأنك لن تحتاج إلي الأسلاك؛ فقط اتصل بنقطة وصول، ويمكنها أن تزود خدمة لعدة كمبيوترات.**
- **حركة – تعزز إنتاجية المستخدم مع إراحته بتمكينه من الاتصال بالشبكة لاسلكياً من أى نقطة ضمن نطاق نقطة وصول.**
- **نشر سريع ومرن – مدد شبكة سلكية بسرعة مع سهولة إرفاق نقطة وصول باتصال شبكي مرتفع السرعة.**
- **البرامج – كملحق للشبكة السلكية، تعمل الشبكات WLAN مع كل البرامج الموجودة. البروتوكول القياسي TCP/IP، مدعوم في كل أشكال اللاسلكي.**
- **الأداء – تقدم الشبكات WLAN اتصالاً مرتفع السرعة بينما يساوي الإيثرنت، بدأ يصبح أسرع منه بشكل متسارع .**

لقد بدأ الأفراد والشركات على حد سواء يدركون فوائد الشبكات WLAN ، ويتوقع في القريب العاجل ، أن تعتمد أكثرية الشركات على التقنية اللاسلكية لتلبية احتياجاتها المهنية والتشبيكية .

اللاسلكي يساوي تردد الراديو

المفهوم التقني الأول الذي تحتاج إلي فهمه عند مناقشة ما الذي يشكل تهديداً لشبكة لاسلكية هو أن الشبكات **802.11** تستعمل ترددات الراديو لإرسال البيانات جيئة وذهاباً بين نقاط النهاية، تماماً كالهواتف اللاسلكية أو أجهزة الراديو التي لديك في المنزل. الفرق الرئيسي هو التردد الذي تُرسل به الإشارات .

يمكن أن تسافر موجات الراديو مسافات طويلة، بناءً على التردد الجارى استخدامه. يمكن لبعض الترددات أن تسير **90-120** متراً، ويتطلب تحقيق ذلك طاقة قليلة. معظم الهواتف اللاسلكية وبطاقات الشبكة اللاسلكية الأقدم تستعمل التردد **900** ميجاهرتز كموجة حاملة، ويمكن لهذه أن تسافر أبعد بقليل مما يدرك معظم الأشخاص. ليس أمراً مستغرباً أن يعطى الهاتف اللاسلكي **900** ميجاهرتز المستخدم مجال استعمال يصل إلي شارع أو شارعين على الأقل قبل أن تفقد السماعة اتصالها بالوحدة القاعدة. شارع أو شارعين يعني **120-150** متر تقريباً.

إذا كانت سماعة هاتفك قادرة على البث بما أقصاه **150** متر هذا يعني أن اتصالك اللاسلكي قادر على مسافات مشابهة. إذا كانت لديك نقطة وصول لاسلكي (**Wireless Access Point** أو **WAP**) مثبتة في مكتبك أو منزلك، كن متأكداً أن الأشخاص الذين يسيرون في الخارج يقعون ضمن نطاقها التشغيلي. يصح نفس الشيء إذا كانت لديك نقطة **WAP** مثبتة في شبكة مكتبك الصغير أو مكتبك المنزلي. إذا تم تثبيت نقطة **WAP** اعتيادية في غرفة جلوسك وكنت تقيم في مبنى فيه عدة شقق، من الممكن جداً أن تكون تزود خدمة الانترنت لمعظم الشقق حتى دون أن تدرك ذلك.

تغطية الشبكات اللاسلكية

كل نقطة وصول لاسلكي لها نطاق محدود يمكن ضمنه المحافظة على اتصال لاسلكي بين كمبيوتر العميل ونقطة الوصول. تختلف المسافة الفعلية بناءً على البيئة؛ يذكر الصانعون عادة النطاقات داخل المنزل وفي الهواء الطلق لإعطائك فكرة معقولة عن الأداء الموثوق به.

انتبه أيضاً إلي أنه عند العمل عند حافة حدود النطاق، قد ينخفض الأداء بسبب تدهور نوعية الإشارة اللاسلكية.

الشبكات اللاسلكية تعمل على مدى محدود نسبيا، حيث يصل أقصى مدى تمتد إليه الشبكات العاملة بمعيار 802.11b داخل مكان مغلق إلي ٤٥–٩٠ متر وربما يصل مدي الشبكات اللاسلكية في الهواء الطلق إلي مسافة ٣٠٠ متر، لكن مرة أخري هذا يعتمد علي المكان والبيئة. ولكن هذه المسافة نظرية إلي حد ما ويرد عليها بعض القيود التى تقلصها إلي مسافة أقل من ٤٥–٩٠ متر والمثال على ذلك إذا كانت شبكة لاسلكية تحتوى على ثلاثة أجهزة محمولة الأول يعمل عليه عمر والثانى مخصص لشخص اسمه حمزة والثالث لشخص اسمه ميسرة افرض أن جهاز عمر يبعد عن جهاز حمزة بمسافة قدرها ٦٠ متر ويبعد جهاز حمزة عن جهاز ميسرة بمسافة قدرها ٦٠ متر أيضا فى الجهة المقابلة (انظر شكل ٢٧–١) فى هذه الحالة يمكن لجهاز حمزة الاتصال بنجاح بكل من عمر ، وميسرة، حيث تبعد المسافة بينه وبين كل منهما بمسافة قدرها ٦٠ متر. ولكن لا يمكن لكل من عمر و ميسرة الاتصال ببعضهما حيث تزيد المسافة بينهما عن ٩٠ متر وبالتالي يقعان خارج المدى المحدد للشبكة



شكل ٢٧–١ تغطية الشبكات اللاسلكية.

هناك قيد آخر على المدى الذى تصل إليه الشبكات اللاسلكية حيث يقل هذا المدى عمليا. يقل المدى الفعلى المخصص لبطاقة الشبكة اللاسلكية عن المدى المحدد نظريا بفعل بعض المعوقات التى تقع فى مدى الشبكة مثل الحوائط أو الأحوال الجوية السيئة أو تداخل الإشارات اللاسلكية مع إشارات التليفونات المحمولة ، والقيد الثالث الذى يعوق اتصال الشبكات اللاسلكية فى حدود الــ ٩٠متراً. إذا كان الجهاز المعدنى الذى يقوم بإرسال واستقبال الإشارات الكهرومغناطيسية Antenna غير مضبوط جيدا.

من الجدير بالذكر أيضا أن سرعة الشبكات اللاسلكية تنخفض كلما زادت المسافة التى تغطيها مثلا . تعمل أجهزة الشبكة التى تعمل بمعيار 802.11b بسرعة نظرية تصل إلي ١١ ميجابت فى الثانية (11Mbps). ولكن الواقع يقول أن هذه السرعة تعمل فقط إذا كانت المسافة إلي حوالى ٤٥ متر فقط. أما إذا امتدت المسافة بين جهازين داخل الشبكة إلي ٩٠ متر فإن سرعتها تنخفض إلي ١ ميجابت فى الثانية (1 Mbps) إذا حاولت الاتصال من مسافة تتجاوز المدى المحدد للشبكة اللاسلكية وربما ينقطع الاتصال.

بطاقات الشبكة اللاسلكية

كما هو الحال فى الشبكات المحلية LAN والشبكات الموسعة WAN تحتاج الشبكات اللاسلكية إلي بطاقات شبكة. ولكنه يختلف عن ذلك المستخدم فى شبكات LAN حيث :

يلزم استخدام كارت شبكة لاسلكية Network Interface Card (NIC) لكل جهاز كمبيوتر متصل بشبكة لاسلكية حتى يتم الاتصال.

يوجد فى بطاقة الشبكة اللاسلكية جهاز معدنى لإرسال واستقبال الإشارات الكهرومغناطيسية بدلا من موصل الكابل فى خلف NIC. ورغم أن تكلفة بطاقة الشبكات اللاسلكية مرتفعة إلا أنها توفر ثمن الكابلات وتثبيتها.

توجد أنواع مختلفة من بطاقات الشبكة اللاسلكية، يمكنك اختيار ما يناسبك منها حسب متطلبات النظام نوع جهاز الكمبيوتر المستخدم.

وصل الشبكات اللاسلكية

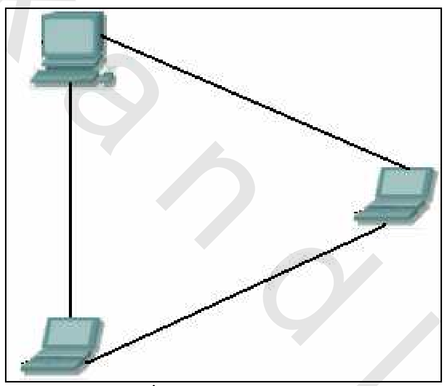
يتم الاتصال بين الأجهزة فى شبكات LAN باستخدام جهاز توصيل HUB أو مبدل Switch.

فى الشبكات اللاسلكية لايلزمك أى من هذين الجهازين، يكفى أن تشترى بطاقة شبكة لاسلكية لكل جهاز كمبيوتر مع وضع الأجهزة كلها فى مدى ٣٠٠ قدم من بعضها البعض.

أما إذا كان عندك شبكة سلكية وتريد إضافة أجهزة أخرى إلي الشبكة لاسلكيا، فيلزمك شراء موصل أجهزة الكمبيوتر اللاسلكية بالشبكة السلكية، يستخدم لهذا الغرض جهاز

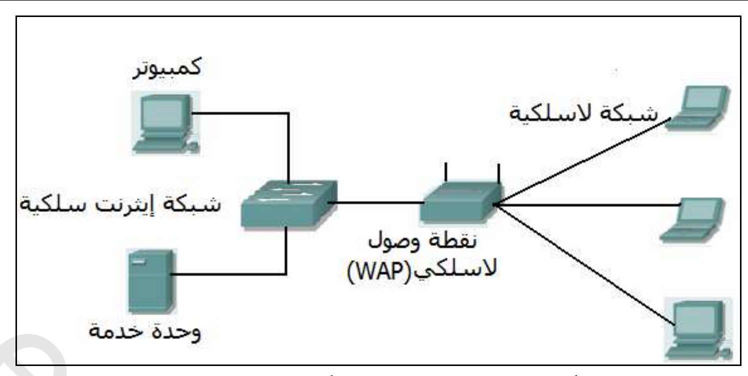
يسمى Wireless Access Point أو WAP. من هذا نفهم أن هناك طريقتان ممكنتان من الشبكات اللاسلكية. ويختلفان حسب الطريقة التي تتصل بها الأجهزة اللاسلكية بعضها البعض علي النحو التالي:

الطريقة الأولي : وهي التشبيك المنشأ لغرض خاص ويعرف أيضاً بالتشبيك اللاسلكي نظير لنظير. كما هو مبين في شكل ٢٧-٢. وفي هذا الشكل توجد ثلاثة كمبيوترات لاسلكية تحتاج لإرسال بيانات إلي بعضها البعض. تسمي هذه الطريقة "مجموعة الخدمة الأساسية المستقلة" (IBSS). يستطيع كل كمبيوتر أن يتصل بكل الكمبيوترات اللاسلكية الأخرى مباشرة. ويمكنها أن تشارك ملفات وطابعات بهذه الطريقة ولكنها لا تستطيع الوصول إلي موارد شبكة LAN في حالة وجودها.



شكل ٢٧-٢ التشبيك اللاسلكي المُنشأ لغرض خاص

الطريقة الثانية : تتطلب هذه الطريقة من التوصيل نقطة وصول لاسلكي Wireless Access Point أو WAP. نقطة الوصول مطلوبة ليس فقط للسماح للكمبيوترات اللاسلكية بالاتصال ببعضها البعض، بل أيضاً للاتصال بشبكة سلكية كما هو مبين في شكل ٢٧-٣. معظم شبكات WLAN تعمل بهذه الطريقة. وتسمي هذه الطريقة "البنية التحتية" لأنها تتطلب وصولاً إلي شبكة LAN السلكية لاستعمال خدمات كالطابعات وخادمات الملفات.



شكل ٢٧-٣ التشبيك اللاسلكي ذو البنية التحية

يشتمل الشكل على شبكة سلكية تحتوى على جهازى كمبيوتر مرتبطين بواسطة سويتش ولأننا نرغب فى إضافة جهازى كمبيوتر محمول وجهاز آخر مكتبي **Desktop** إلي الشبكة اللاسلكية. قمنا بتوصيل جهاز السويتش بجهاز **WAP** الذى يتمكن بدوره من وصل الأجهزة اللاسلكية.

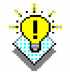
Wireless Access Point عبارة عن جهاز على شكل صندوق به جهاز معدنى (أو جهازين) لإرسال واستقبال الإشارات الكهرومغناطيسية ومنفذ **RJ-45**. يتم ربط **WAP** بكابل الشبكة وإدخال الطرف الآخر من الكابل فى جهاز سويتش أو **hub** . وبذلك تتصل الشبكة اللاسلكية بأخرى سلكية.

التشبيك اللاسلكي

يشير المصطلح تشبيك لاسلكى (**Wireless Network**) إلي تقنية الراديو التي تمّكن كمبيوترين أو أكثر من الاتصال باستعمال بروتوكولات الشبكة القياسية ك **IP**، لكن من دون كبلات. تتطلب أجهزة التشبيك اللاسلكي استعمال تقنية تتعاطى مع ترددات الراديو وإرسال البيانات. المعيار القياسي الأكثر استعمالاً هو **802.11**، هذا هو المعيار القياسي الذي يعرف كل نواحي التشبيك اللاسلكي ذي تردد الراديو .

يحدد **802.11b** أن أجهزة الراديو تتكلم على النطاق **2.4** جيجاهرتز غير المرخص بسرعة إرسال تبلغ **11** ميجابت بالثانية في إحدى الأقنية الـــ **15** الخاصة. تبحث بطاقات الشبكة اللاسلكية بين تلك الأقنية تلقائياً لإيجاد الشبكات **WLAN**، لذا لا حاجة لضبط

تكوين محطات العملاء عند أقنية معينة. عندما تجد بطاقة الشبكة القناة الصحيحة، تبدأ التكلم مع نقطة الوصول. طالما كانت كل إعدادات الأمان لدى العميل ونقطة الوصول متطابقة، يمكن أن تبدأ الاتصالات عبر نقطة الوصول، ويستطيع المستخدم أن يشارك كجزء من الشبكة.



802.11g هو معيار لاسلكي جديد مرتفع السرعة يتيح للمستخدمين إرسال البيانات بسرعات تصل إلي **54** ميجابت بالثانية – تقريباً خمس مرات أسرع من التقنية **802.11b** لأن **802.11g** يعمل في نطاق الترددات **2.4** جيجاهرتز فإنه متوافق كلياً مع **802.11b** ومتوفر ليستعمل في جميع أنحاء العالم. حالياً، تدعم شركة أبل المعيار **802.11g** في كل أجهزتها، وستلحقها سيسكو قريباً .

الشبكات اللاسلكية الكبرى

يمكن استخدام اثنين أو أكثر من **Wireless Access Point (WAP)** لإنشاء شبكة لاسلكية كبرى تسمح لمستخدميها بالتجوال من مكان لآخر مع استمرار إمكانية اتصالهم بالشبكة. والفكرة أن المستخدم عندما ينتقل خارج المدى المخصص لــ **WAP** تلتقطه **WAP** أخرى وتحل محل **WAP** الأولى بدون أن تنقطع خدمة الاتصال المتاحة للمستخدم. لإعداد اثنين أو أكثر من **WAP** ولكى تتحقق خاصية التجوال يجب تحديد مواقع **WAPs** بدقة بحيث تقع كل المسافة التى ترغب فى مد خدمة التجوال إليها فى المدى المحدد لواحد على الأقل من **WAP** . لابد أن تتأكد أن جميع أجهزة الكمبيوتر و **WAPs** تستخدم نفس **SSID** ونفس قناة الاتصال.

اتصال أكثر من شبكة

افرض أن شركتك تستخدم شبكتين منفصلتين فى مكانين مختلفين بنفس المبنى. وأنه يصعب الربط بينهما بكابلات. الحل الأمثل فى هذه الحالة هو استخدام اثنين من **Wireless Access Point** لإنشاء ما يسمى بقنطرة لاسلكية (جهاز وصل لاسلكى) بين الشبكتين. وصّل أحد **WAPs** بالشبكة الأولى والآخر بالشبكة الثانية. ثم قم بتوصيل كلا من **WAPs** لاستخدام نفس **SSID** ونفس قناة الاتصال.

التهديدات اللاسلكية

تأتي التهديدات اللاسلكية بكل الأشكال والأحجام، من شخص يرتبط بنقطة وصولك اللاسلكي من دون ترخيص، إلي التقاط رزم من الهواء وفك تشفيرها من خلال شمام رزم "Packet Sniffer" . لا يملك الكثير من المستخدمين اللاسلكيين أي فكرة عن أنواع الأخطار التي تواجههم بمجرد ربطهم نقطة وصول لاسلكي بشبكتهم السلكية. نوضح فيما يلي التهديدات الأكثر شيوعاً عند إضافة مكون لاسلكي إلي شبكتك.

الطبيعة الجوية لإرسالات الشبكة **WLAN** تعرض شبكتك للمقتحمين والهجمات التي يمكن أن تأتي من أى اتجاه. تسافر حركة مرور الشبكة **WLAN** على موجات الراديو التي لا تستطيع جدران المباني أن تكبحها كلياً. رغم أن الموظفين قد يتمتعون بالعمل على كمبيوتراهم المحمولة من مكان طبيعي خارج المبنى، إلا أنه بإمكان المقتحمين والقراصنة الوصول إلي الشبكة من موقف السيارات أو من الشارع باستعمال هوائي علبة البرينجلز.

كيف يتم اختراق الشبكة اللاسلكية

لا يلزم فى حالة الشبكات اللاسلكية أن ينجح المخرب في الوصول إلي جهاز الكمبيوتر فى شركتك حتى يخترق الشبكة ، حيث يمكن التسلل إلي الشبكات من خلال وسيلة تعرف بـــــ"التوجيه اللاسلكي ".وفكرة التوجيه اللاسلكي تتلخص فى استخدام جهاز كمبيوتر محمول لاسلكي للبحث عن شبكات لاسلكية غير مؤمنة والاتصال بها .

يجهز الهاكرز أجهزهم بهوائيات لاسلكية خارجية لتسهيل مهمة الحصول علي النقاط الفعالة اللاسلكية ويلجأون في الغالب الي استخدام جهاز يدوي يسمي **Global Positioning System** او **GPS** وتعني (نظام تحديد مواضع عامة) لمساعدهم في تعيين الحدود الفعلية للنقط الفعالة .

بمجرد إيجاد نقطة فعالة لاسلكية غير مؤمنة ، يستطيع الهاكرز الوصول مجاناً إلي الانترنت . بل أنهم يقومون أكثر من ذلك بإرسال معلومات عن النقاط الفعالة الي غيرهم من المخربين الذي يستخدمون التوجيه اللاسلكي من خلال بعض المواقع علي الويب .

بل إن الأمر يصل بالبعض منهم إلي التجوال بسيارهم في المدينة ومعهم أجهزهم المحمولة بحثاً

عن أي اتصال مفتوح بشبكة لاسلكية .

يستخدم الهاكرز مصطلح **War driving** للإشارة إلي أدوات اختراق الشبكات اللاسلكية . إذا بحثت عن كلمة **War Driving** باستخدام احد محركات البحث، ستجد الكثير من المواقع تحتوي علي عدد كبير من الأدوات للتسلل علي الاتصالات اللاسلكية .

ولكن ليس بالضرورة أن يقتحم المخربون أو "الهاكرز" الشبكات اللاسلكية بواسطة التوجيه اللاسلكي. إن الأمر أصبح أسهل من ذلك بكثير لأن الاتصال اللاسلكي عبارة عن بث علي موجات الراديو، ولذلك فبإمكان الأشخاص الذي يتنصتون علي الإرسالات اللاسلكية أن يلتقطوا الرسائل غير المشفرة بسهولة. وهذا خلافاً لشبكات **LAN** السلكية. في الحقيقة أن مستخدم شبكة **WLAN** ليس محصوراً بالمنطقة الجغرافية للشركة، أو بنقطة وصول واحدة. يمكن أن يمتد نطاق شبكة **WLAN** إلي خارج الحدود الجغرافية للمكتب أو المبني، مما يسمح للمستخدمين غير المرخص لهم بالوصول من مكان عام أو من غرفة مكتب مجاور. المخرب الذي يستهدف نقطة **WAP** غير محمية، يحتاج فقط أن يتواجد إلي جوار الهدف، ولم يعد اليوم إلزامياً أن يمتلك مهارات متخصصة أو التوجيه اللاسلكي لكي يقتحم الشبكة. كثيراً ما تجد في الشبكات اللاسلكية لأحد أمرين:

- شركة مجاورة لديها شبكة لاسلكية مفتوحة.
- مستخدم مجاور قد انضم إلي شبكة لاسلكية شغالة.

الاختراق بالتقاط الرزم

أفضل وسيلة لفحص البيانات التي تخرج عبر اتصال ايثرنت (سلكي أو لاسلكي) هي استخدام برنامج **Packet Sniffer** أو "شمام الرزم". وهو برنامج يتيح التقاط كل الرزم الخارجة عبر اتصال ايثرنت واحد أو عدة اتصالات لفحصها لاحقاً. تلك البرامج الشمامة تمسك الرزمة وتحللها، وتكشف حمولة البيانات المتواجدة فيها. توجد بعض برامج شمام الرزم مجانية مثل برنامج **Ethereal** ولأن الشبكة اللاسلكية لا ترسل أي شئ مشفر، ترسل البيانات كنص عادي. المهاجم الذي يملك شمام الرزم يستطيع الآن أن يسرق هوية المستخدم ويسجل دخوله إلي خادم البريد بصفته المستخدم المرخص له.

أظن أنك الآن وبعد أن قرأت عن التقاط الرزم، قد أحسست بالرعب عند معرفتك أن هناك شمامات متوفرة بسهولة للشبكات اللاسلكية وبعضها مجاني. تخيل مدي الخطورة إذا كنت تسجل دخولك إلي الميدان وتفحص حسابك المصرفي وما هو حجم الخسارة التي ستلحقك إذا أختطف أي من المخربين هذه المعلومات.

كيف نحمي الشبكة اللاسلكية

فيما يلي بعض الإرشادات التي قد تعينك علي حماية الشبكة اللاسلكية.

- تستخدم الشبكات اللاسلكية جهاز يسمي **Wireless Access Point** وتختصر هكذا **WAP** لوصل أجهزة الكمبيوتر اللاسلكية بالشبكة السلكية الموجودة بالفعل . لذلك يجب عليك تنشيط سمة **Wired Equivalent Privacy** وتختصر **WEP** لجميع الأجهزة اللاسلكية في شبكتك . تعمل سمة **WEP** علي تأمين البيانات المنقولة في الشبكات اللاسلكية . ورغم أن هذه السمة لا توفر حماية تامة للبيانات إلا أنها تمنع محاولات التسلل المعتاد إلي الشبكة .
- تستخدم الشبكات اللاسلكية ما يعرف بــ **Service Set Identifier** وتختصر هكذا **SSID** ومعناها (معرف محدد الخدمة) لتعريف الشبكة اللاسلكية . بعبارة أخري يستخدم كاسم للشبكة اللاسلكية . يتم الاتصال بنقاط الوصول للشبكة اللاسلكية عن طريق **SSID** بواسطة أجهزة كمبيوتر محمولة .

يوصف كل مورد نقطة وصول نقاط الوصول الخاصة به باستخدام **SSID** افتراضي ويعرف الهاكرز ما هية معرفات **SSID** الافتراضية لمعظم نقاط الوصول للشبكة . لحماية شبكتك قم بتغيير القيم الافتراضية لــ **SSID** .

ولكننا ننصحك ألا تعول كثيراً علي تغيير **SSID** لأن التغيير لن يحمي الشبكة كثيرا.

- احذر من تثبيت أجهزة **Wireless Access Point** بخلاف تلك التي قمت بنفسك بتثبيتها على الشبكة. نظرا لانخفاض أسعار **WAP** وسهولة تثبيتها فقد يقوم أحد المستخدمين بتثبيت أحدها على الشبكة بدون إذن من مديرها. قد تعرض هذه الأجهزة الشبكة بالكامل للخطر .

- قم بتغيير جميع كلمات المرور الافتراضية، خاصية كلمات مرور **WAP** وحقوق دخول مدير الشبكة، وذلك لجميع وحدات الخدمة
- ترجع معظم حالات فشل الخطط التأمينية لأجهزة الكمبيوتر إلي استخدام كلمات مرور غير قوية.

ملخص الفصل

ألقينا نظرة علي الشبكات اللاسلكية باعتبارها حالياً من الخيارات الفعالة في مجال الشبكات لأنها تتطور بشكل هائل وتنخفض أسعار منتجاتها أيضا. شرحنا في هذا الفصل مزايا الشبكات اللاسلكية وفكرة عملها. شرحنا معيار **802.11** باعتباره المعيار القياسي للإرسال اللاسلكي في الشبكات اللاسلكية ، وتعرضنا لمجال تغطيتها.

شرحنا بعد ذلك بطاقة الشبكة اللاسلكية وكيفية وصل الشبكات اللاسلكية العادية أو الشبكات اللاسلكية الكبرى ، أخيراً شرحنا التهديدات التي تواجه الشبكات اللاسلكية وختمنا ببعض الإرشادات التي تعينك علي حماية الشبكة اللاسلكية .

تدريبات

١. ما هي العوامل التي تؤثر في المدي الفعلي المخصص لبطاقة الشبكة اللاسلكية عن المدي المحدد نظرياً؟

٢. صح أم خطأ

أ. لا تؤثر البيئة أو المكان علي مدي تغطية الشبكات اللاسلكية.

ب. المصطلح **Wi-Fi** مرادف لمصطلح الشبكات اللاسلكية.

ج. المدي الذي تغطيه الشبكات اللاسلكية ثابت في كل الأحوال والظروف.

د. لتوصيل أجهزة كمبيوتر إلي شبكة موجودة لاسلكياً، يلزمك شراء جهاز يسمي **WAP** .

٣. أذكر ثلاثة أسباب تدعوك لاقتناء شبكة لاسلكية .

٤. ما هو الاختلاف والتشابه بين المصطلح **802.11** والمصطلح **Wi – Fi** ؟

٥. أذكر أحد برامج شمام الرزم المجانية ؟

٦. صح أم خطأ

أ. الشبكات اللاسلكية محصنة أمام نفس أنواع هجمات الحرمان من الخدمة كالشبكة السلكية.

ب. الشبكات اللاسلكية سريعة التأثر بالهجمات التي تتدخل بإشارات الراديو كالتشويش.

ج. تغيير إعدادات SSID الافتراضية من حين لآخر يقلل من مخاطر التهديدات اللاسلكية .





الفصل الثامن والعشرون

الشبكات VPN

*إن أكثر موضوع تداولاً في أمان البيانات هذه الأيام ، الشبكات الخصوصية الوهمية (الشبكات **VPN**) وهي تقنية واعدة ومهمة جداً للشركات التي تسعي إلي تخفيض التكلفة وزيادة المرونة وقابلية التحجيم وضمان أمان اتصالاتها. بانتهاء هذا الفصل ستتعرف علي :*

- *استعمال الشبكات **VPN** وكيف تعمل.*
- *أنواع الشبكات **VPN**.*
- *فوائد الشبكات **VPN**.*
- *التشفير الذي يزوده **IPSec**.*
- *كيف تضمن **VPN** المحافظة علي أمان شبكتك.*
- *البروتوكولات المستخدمة خلال شبكة **VPN IPSec**.*

مقدمة

مع نمو حجم الاتصال وازدياد معدل التنقل الشخصي ، تزداد أيضاً الحاجة للشبكات من أجل التكيف وتزويد خدمات. لا يفهم المستخدمون الهموم الأمنية للخدمات البعيدة التي يتطلبونها للإنتاجية، المستخدمون الذين يسافرون إلي بلدان أخري، في المطارات ، مواقع العملاء...الخ . يلزمهم الاتصال بموارد الشركة لكي ينجزوا أعمالهم. مع المستويات المتزايدة لنوعية الاتصال من T1 واللاسلكي في المطارات ، إلي العملاء ذوي الاتصالات المرتفعة السرعة، يواجه المسئولون عن صيانة الشبكات السؤال التالي. كيف يجب عليهم تزويد المستخدمين بخدمات تكنولوجيا المعلومات المطلوبة، بغض النظر عن مكانهم، بأسلوب آمن ومعقول؟

والحل الرائد لهذه الطلبات هو "بروتوكول أمان بروتوكول الانترنت" (Internet Protocol Security Protocol) أو IPSec الملقّب بـــ "الشبكات الخصوصية الوهمية" (أو الشبكات VPN).

لكن ما الذي تفعله الشبكة VPN بالضبط، وكيف يمكنها أن تؤثر علي أعمال شركتك ؟ إن شعبية تقنية الشبكة VPN مرتبطة مباشرة بإمكانيتها علي إعطاء عائدات كبيرة علي الاستثمار للشركات التي تدفع التكاليف الباهظة في أغلب الأحيان للاتصالات الخصوصية عبر الخطوط المؤجرة ، عند نشر شبكات VPN لاستبدال تلك الاتصالات المكلفة يصبح التوفير في التكاليف كبيراً.

التقنيات التي تستبدلها الشبكات VPN في معظم الأحيان هي :

- تحل الشبكات VPN بين المواقع (Site – to – Site) محل الشبكات الواسعة (الشبكة WAN) المكلفة عن طريق استبدال خدمات الخط الخصوصية بالشبكات VPN التي تستعمل الانترنت بدلاً منها.
- تزيل أو تقلل الشبكات VPN للوصول عن بعد بشكل كبير تكاليف المكالمات الهاتفية البعيدة المسافة للاتصال بمندوبي المبيعات البعيدين أو المكاتب الصغيرة .

إذا كانت مؤسستك تستثمر مبالغ كبيرة بشكل متكرر إما علي الشبكة WAN أو علي

تكاليف المكالمات الهاتفية البعيدة المسافة ، فإن شبكة VPN يمكن أن تكون أسلوباً بديلاً ذي فائدة كبيرة بكلفة أقل ومرونة أكثر.

نظرة عامة علي الشبكة VPN

الشبكة الخصوصية الوهمية (الشبكة VPN) هي اتصال شبكي مشفر يستعمل نفقاً آمناً بين نقاط نهاية عبر الانترنت أو شبكة أخري، كشبكة WAN. في الشبكة VPN تحل الاتصالات المحلية بمزود خدمة الانترنت (ISP) محل الاتصالات الهاتفية بالمستخدمين البعيدين أو اتصالات الخط المؤجر بالمواقع البعيدة.

السيطرة المتزايدة لاتصالات الانترنت العريضة النطاق بالمكاتب البعيدة الصغيرة بالمنازل تجعل استعمال الوصول الأرخص إلي الانترنت جذاباً. بعد الاستثمار الأوَّلي في الشبكات VPN ، تصبح تكلفة إضافة مزيد من المواقع أو المستخدمين صغيرة جداً.

تتيح الشبكات VPN لكل مستخدم بعيد لشبكتك بأن يتصل بأسلوب آمن وموثوق به باستعمال الانترنت كوسط للاتصال بشبكتك LAN الخصوصية. يمكن أن تنمو الشبكة VPN لتتسع مزيداً من المستخدمين وأماكن مختلفة بسهولة أكبر من الخط المؤجر. في الواقع، قابلية التحجيم هي ميزة رئيسية للشبكات VPN بالمقارنة مع الخطوط المؤجرة النموذجية. في حالة الخطوط المؤجرة تزداد التكلفة كلما زادت المسافة أما في الشبكة VPN فلا تهم الأماكن الجغرافية لكل مكتب .

تتيح الشبكة VPN تمديد شبكة انترانت خصوصية بأمان من خلال تشفير IPSec عبر الانترنت أو خدمة شبكة أخري، مما يسهل التجارة الالكترونية الآمنة واتصالات الاكسترانت مع الموظفين المتنقلين، والشركاء المهنيين والموردين والعملاء.

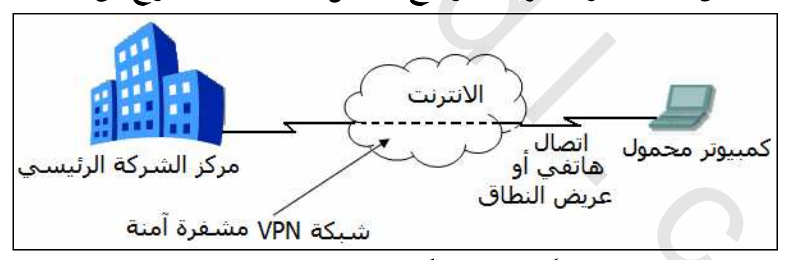
أنواع شبكات VPN

هناك ثلاثة أنواع رئيسية من الشبكات VPN

- الشبكات VPN للوصول عن بعد (Remote Access VPNs) :

تتيح للمستخدمين الهاتفيين الفرديين الاتصال بأمان بموقع مركزي عبر الانترنت أو

خدمة شبكة عمومية أخري. هذا النوع من الشبكات يتيح للموظفين الذين يحتاجون إلي الاتصال بشبكة الشركة من الخارج الاتصال بشبكة LAN . وهؤلاء تستعمل أنظمتهم برنامجاً خاصاً للشبكة VPN يسمح بإنشاء وصلة آمنة بينهم وبين شبكة الشركة. عادة، الشركة التي تريد إعداد شبكة VPN كبيرة للوصول عن بعد ستزود أحد أشكال حساب الانترنت الهاتفي للمستخدمين الذين يستعملون مزوداً. عندها، يستطيع المتصلون عن بعد أن يتصلوا برقم مجاني للوصول إلي الانترنت ويستعملوا برنامج شبكتهم VPN للوصول إلي شبكة الشركة. المثال الجيد عن شركة تحتاج إلي شبكة VPN للوصول عن بعد، شركة كبيرة فيها مئات مندوبي المبيعات في الأسواق. تسمي الشبكات VPN للوصول عن بعد أحياناً بـــ "الشبكات VPN البرمجية" أو "الشبكات الهاتفية الخصوصية الوهمية (VPDN)" أو "الشبكات VPN الهاتفية". يدفع المستخدمون "تكلفة ثابتة" منخفضة لمزود محلي باستعمال مكالمة محلية ولذا لا يتكبدون تكاليف المكالمات الدولية البعيدة المسافة ولا يضطرون إلي فتح مكالمة مباشرة دولية المسافة بمكتبهم في الشركة. يستطيع المستخدم عندها أن يستعمل اتصال المزود المحلي لإنشاء نفق VPN عبر الانترنت. يوضح الشكل ٢٨-١ هذا النوع من الشبكات.

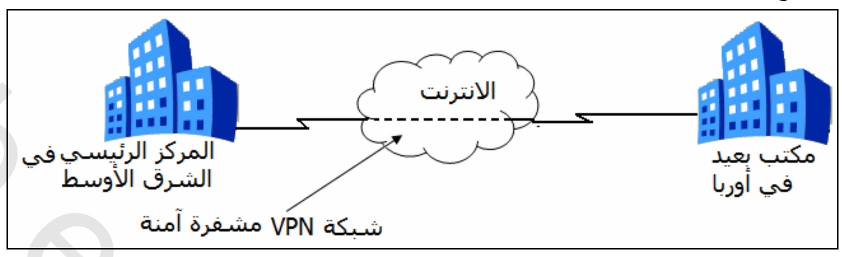


شكل ٢٨-١ شبكة VPN للاتصال عن بعد

- الشبكات VPN بين المواقع (Site – to Site)

تستعمل لتمديد شبكة LAN موجودة لشركة إلي أبنية ومواقع أخري من خلال استعمال معدات مكرسَّة، لكي يتمكن الموظفون البعيدون في تلك الأماكن من أن يستخدموا نفس خدمات الشبكة. تعتبر هذه الأنواع من الشبكات VPN متصلة بنشاط طوال الوقت. تسمي الشبكات VPN بين المواقع أحياناً بالانترنت، أو

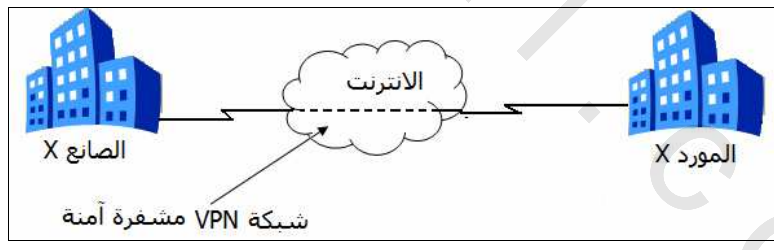
الشبكات VPN بين شبكات LAN . يوضح شكل ٢٨-٢ شبكات VPN بين المواقع.



شكل ٢٨-٢ شبكة VPN بين المواقع

- **شبكات VPN الاكسترانت (Extranet VPNs)**

تتيح إنشاء اتصالات آمنة مع الشركاء المهنيين والموردين والزبائن بهدف إجراء تجارة إلكترونية. شبكات VPN الاكسترانت هي الملحق لشبكات VPN الانترنت مع إضافة جدران النار لحماية الشبكة الداخلية. المثال الجيد هو شركات تعمل بشكل كثيف مع الموردين والشركاء لتحقيق أهداف مشتركة كعلاقات العرض والطلب مثلاً، عندما تحتاج شركة إلي موارد ويلبي المورد طلباتها. بالعمل عبر شبكة اكسترانت ، تستطيع تلك الشركتين أن تتشارك المعلومات بسرعة أكبر. يوضح شكل ٢٨-٣ شبكة VPN الاكسترانت.



شكل ٢٨-٣ شبكة VPN الاكتسترانت

تهدف كل هذه الشبكات VPN إلي زيادة الثقة وتحسين الأداء وأمان لبيئات الشبكة WAN التقليدية باستعمال اتصالات مزودة أو خدمة أخري ذات تكلفة أقل ومرونة أكثر.

في الأشكال الثلاثة السابقة كل الشبكات VPN تستخدم الانترنت. يمكن استعمال تقنية الشبكة VPN أيضاً ضمن شبكتك لتزويد طبقة إضافية من الأمان للتحكم بالوصول إلي

المعلومات أو الأنظمة أو الموارد الحساسة. مثلاً، يمكن استعمال تقنية الشبكة VPN للحد من الوصول إلي الأنظمة المالية عند بعض المستخدمين أو لضمان إرسال المعلومات الحساسة أو السرية بطريقة آمنة . في هذا السيناريو ، بإمكان الشبكات VPN أن تشفر نقل البيانات إلي الأنظمة الحساسة وتحميها أكثر فأكثر.

فوائد وأهداف الشبكة VPN

يمكن إجمال فوائد تطبيق شبكة VPN في شبكتك فيما يلي :

- *تخفيض تكاليف الاتصالات*: قبل ظهور الشبكة VPN، كان الموظفون في الأماكن البعيدة يضطرون إلي إجراء مكالمات هاتفية بعيدة المسافة (دولية) للوصول إلي شبكة شركتهم. يمكن تخفيض تكاليف الاتصالات عن بعد نتيجة استبدال الاتصالات الهاتفية البعيدة المسافة باتصالات محلية بالانترنت التي يمكن من خلالها أن يستعمل المستخدمون شبكة VPN. بناء علي عدد الموظفين أو المندوبين في الأسواق، يمكن أن يشكل هذا لوحده وفراً كبيراً في التكلفة . بالنسبة للعديد من الشركات الصغيرة ذات الميزانية المحدودة، يمكن أن يشكل مزودو الشبكة VPN حلاً عملياً .
- *زيادة الإنتاجية* : زيادة إنتاجية المستخدمين بتمكينهم من الوصول إلي موارد الشبكة بأمان بعض النظر عن مكانهم الجغرافي.
- *تخفيض التكاليف التشغيلية* : المقترنة باتصالات الشبكة WAN المكرسة باستبدالها باتصالات مباشرة بالانترنت كالاتصال العريض النطاق الخاص بالشركات، الذي من خلاله ستتصل المواقع البعيدة عبر شبكة VPN بين المواقع.
- *تبسيط طوبولوجيا شبكتك* : بإضافة شبكات VPN استراتيجياً في كل أرجاء شبكتك.
- *زيادة الإيرادات*: باستعمال شبكات VPN، ستكسب عائدات أسرع علي الاستثمار من حل الشبكة WAN التقليدية .
- *تحقيق مرونة أكبر :* بسبب نشر الاستخدام المتنقل للكمبيوتر، والاتصال عن بُعد،

وتشبيك مكاتب الفروع، تجارة إلكترونية أسهل واتصالات اكسترانت مع الشركاء المهنيين ، وصول خارجي للموردين والعملاء إلي الانترنت، ووصول داخلي إلي الانترانت والاكسترانت يمكن تزويدها باستعمال اتصال آمن واحد.

- *إتاحة الفرصة للعمل في المنزل:* تخفيض تكاليف المكتب بجعل المستخدمين يعملون من منزلهم. للمستخدمين المنزليين عادة إنتاجية أعلي وضغوط أقل .

استراتيجيات تطبيق الشبكة VPN

بسبب عدم وجود معيار قياسي مقبول بشكل واسع لتطبيق الشبكة VPN، فقد طورت عدة شركات حلولاً جاهزة للعمل من تلقاء نفسها. نوضح فيما يلي بعض المكونات التي تتوفر من سيسكو، وكيف يمكن استعمال الأجهزة ذات الوظيفة الواحدة كجدران النار لتحقيق دور الشبكة VPN :

- *جدران النار* : إذا لم يكن لديك جدار نار قبل قراءة الفصل الخامس والعشرون "جدران النار" الأرجح أنه لديك واحد الآن. جدران النار حاسمة لأمان شبكتك. اليوم، كل جدران نار سيسكو تدعم دمج الشبكات VPN .
- *الموجهات القادرة علي VPN* : يمكن ترقية موجهات سيسكو لإعطائها القدرة علي استعمال الشبكات VPN .
- *مركّز الشبكة VPN* : (VPN Concentrator) جهاز دوره الوحيد في الشبكة هو السماح لشبكات VPN بالاتصال به، وبالتالي السماح للمستخدمين بالوصول إلي بقية موارد الشبكة ، يتم بناء مركزات VPN من سيسكو خصيصاً لإنشاء شبكات VPN لمستخدمي الوصول البعيد، التي تزود أداء مرتفعاً، وقابلية تحجيم، وتتضمن مكونات تدعي وحدات لمعالجة التشفير القابل للتحجيم (SEP)، التي تمكن مهندسي الشبكة من زيادة السعة والإنتاجية بسهولة.
- *برنامج العميل* : سهل نشره وتشغيله، ينشئ برنامج عميل VPN من سيسكو (أو Cisco VPN Client) أنفاقاً آمنة طرفاً لطرف إلي أجهزة الشبكة VPN المذكورة

هنا. هذا البرنامج المتوافق مع **IPSec** ذي التصميم الرفيع يمكن ضبط تكوينه مسبقاً لعمليات النشر الضخمة، وتتطلب تسجيلات الدخول الأولية تدخلاً قليلاً من المستخدم.

بناء علي نوع الشبكة **VPN** (للوصول عن بعد أو بين المواقع)، يجب أن تستعمل أجهزة معينة لكي تبني شبكتك **VPN**. لكن يجب أن تفكر بالأمور التالية أيضاً:

- *سهولة الإدارة* : سهولة إدارة الشبكة **VPN** تهتم بالجهد المطلوب للمحافظة بنجاح علي وصلة الشبكة المنشأة.
- *قابلية التحجيم* : مع نمو أعمال الشركة، وهذا ما يحصل غالباً، تنمو متطلباتها لتكنولوجيا المعلومات ايضاً. لتكبير البنية التحتية لشبكة **VPN** بسرعة وبشكل فعال من حيث التكلفة ، من المهم اختيار حل فيه قابلية تحجيم. فآخر شئ يريده مدير تكنولوجيا المعلومات هو البدء من الصفر واستبدال البنية التحتية لشبكة **VPN** بسبب وجود اختناق في احتمال نموها.

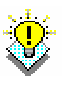
نظرة عامة علي شبكات IPSec الخصوصية الوهمية

لقد أصبح **IPSec** المعيار القياسي لإنشاء الشبكات **VPN** في عالم التشبيك. لقد طبقه كثير من الشركات ولأن فريق عمل هندسة الانترنت (**IETF**) قد عَّرف **IPSec** في مستند **RFC** فإن **IPSec** يعتبر أفضل خيار لبناء الشبكات **VPN**. يقدم **IPSec** وسيلة قياسية لإنشاء خدمات التحقق من الصحة والتشفير بين النظراء. لتبسيط هذه المناقشة، نظراء **IPSec** هم أجهزة تشكل كل طرف لنفق الشبكة **VPN**. يعمل **IPSec** في طبقة الشبكة للنموذج **OSI** المرجعي، فيحمي رزم **IP** ويتحقق من صحتها بين أجهزة **IPSec** المشاركة (النظراء) كموجهات أو جدران نار سيسكو. يزود **IPSec** خدمات أمان الشبكة التالية :

- سرية البيانات : يستطيع مرسل **IPSec** أن يشفر الرزم قبل إرسالها عبر شبكة. إذا لم يكن القرصان قادراً علي قراءة البيانات، لن تكون مفيدة له.
- سلامة البيانات : تتحقق نقطة نهاية **IPSec** المستلمة من صحة الرزم التي يرسلها

مرسل IPSec لضمان أنه لم يتم العبث بالبيانات خلال الإرسال.

- التحقق من أصل البيانات : يستطيع متلقي IPSec أن يتحقق من صحة مصدر رزم IPSec المرسلة. تعتمد هذه الخدمة علي خدمة سلامة البيانات.
- محاربة التكرار : يستطيع متلقي IPSec أن يكتشف ويرفض الرزم المتكررة.
- يحمي IPSec البيانات الحساسة التي تسافر عبر الشبكات غير المحمية، ويتم تزويد خدمات أمان IPSec في طبقة الشبكة (Network Layer). لذا لست مضطراً إلي ضبط تكوين محطات العمل أو الكمبيوترات أو البرامج الفردية. بإمكان هذه الفائدة أن تحقق توفيراً كبيراً في التكلفة .
- يزود IPSec ميزات أمان محسنة، كخوارزميات تشفير أفضل وتحقق شامل أكثر .
- بإمكان شبكات الشركات المتصلة بالانترنت أن تّمكن وصول VPN آمن ومرن بواسطة IPSec.
- مع تقنية IPSec يستطيع العملاء الآن بناء شبكات VPN عبر الانترنت مع أمان حماية التشفير ضد اختراق السلك أو التصنت أو الهجمات الأخرى التي تتطفل علاي الاتصالات الخصوصية.



فقط الأنظمة المتوافقة مع IPSec يمكنها أن تستفيد من هذا البروتوكول. أيضاً، يجب أن تستعمل كل الأجهزة مفتاحاً مشتركاً، ويجب أن تملك جدران نار كل شبكة أساليب أمان ذات إعداد متشابه.

يزود IPSec خدمات التحقق من الصحة والتشفير لحماية البيانات من الإطلاع عليها أو تعديلها لغير المرخص لهم من أفراد شبكتك أو أثناء إرسالها عبر شبكة غير محمية، كالانترنت العمومية. يستطيع IPSec أن يشفر البيانات بين أجهزة مختلفة مثل :

- موجه إلي موجه.
- جدار نار إلي موجه.
- جدار نار إلي جدار نار.
- مستخدم إلي موجه.

- مستخدم إلي جدار نار.
- مستخدم إلي مركز الشبكة **VPN**.
- مستخدم إلي وحدة خدمة **(Server)**

التحقق من الصحة وسلامة البيانات

يمكن التحقق من صحة المستخدمين من خلال التحقق من هوية نقطتي نهاية الشبكة VPN والمستخدمين الذي يرسلون بياناهم عبر الشبكة VPN. نقطة النهاية يمكن أن تكون عميل VPN أو مركّز VPN أو جدار نار أو موجهاً. التحقق من الصحة هي عملية IPSec التي تحدث بعد تشفير البيانات وقبل فك تشفيرها لدي الطرف المتلقي. إنها وظيفة ضرورية ضمن IPSec لضمان أن الجهة المرسلة والمتلقية هما حقاً صاحبتي الحق في البيانات.

سلامة البيانات هي وظيفة أخري ضمن IPSec، السلامة (Integrity) تعني أنه لم يتم العبث بالرزمة التي يستلمها الطرف المتلقي خلال إرسالها. يتم هذا من خلال استعمال خوارزمية معينة تسمي "بعثرة أحادية الاتجاه".

تمرير البيانات عبر أنفاق Tunneling

الأنفاق هي ما تعتمد عليه الشبكات VPN لإنشاء شبكة خصوصية عبر الانترنت. مبدئياً، إنها عملية أخذ رزمة كاملة من البيانات وتغليفها ضمن رزمة أخري قبل إرسالها عبر شبكة. يجب أن تفهم الشبكة بروتوكول الرزمة الخارجية لدخول الشبكة والخروج منها.

شق الأنفاق المنقسم Split Tunneling

لا تتيح شبكات VPN التقليدية للمستخدمين الوصول إلي موارد الشبكة في قسمهم المحلي في نفس الوقت الذي يكونون فيه متصلين بشبكة VPN الخاصة بشركتهم. هذا الوضع يمثل مشكلة في بعض الحالات. مثلاً إذا أراد شخص الوصول إلي نظام من خلال شبكة VPN وفي نفس الوقت الطباعة علي الشبكة المحلية. لتصحيح هذه المشكلة المحتملة، ثم تقديم ميزة Split Tunneling أو شق الأنفاق.

يعمل شق الأنفاق بشكل جيد مع الشبكات VPN لأنه يمكنك استعمال بروتوكولات

ليست مدعومة علي الانترنت داخل رزمة **IP**، وسيظل بالإمكان إرسالها بأمان. في بداية إرسال نفقي **VPN**، يتم لف (أو تغليف) رزمة بيانات من الشبكة **LAN** المصدر بمعلومات رأس جديدة تتيح للشبكات الوسيطة أن تتعرف عليها وتسلمها. بعد أن يتم هذا ويكتمل الإرسال، يتم نزع "رأس" بروتوكولات شق الأنفاق، وتُرسل الرزمة الأصلية إلي الشبكة **LAN** الوجهة لتسليمها.

رغم أن شق الأنفاق يتيح نقل البيانات عبر شبكات الطرف الثالث، إلا أنه لوحده لا يضمن الخصوصية. لحماية إرسال نفقي من أي اعتراض أو تلاعب، يتم تشفير كل البيانات المنقولة عبر الشبكة **VPN**. بالإضافة إلي ذلك، تتضمن الشبكات **VPN** عادة ميزات إضافية، كجدران النار .

في الشبكات **VPN** بين المواقع، بروتوكول التغليف هو **IPSec** عادة أو تغليف التوجيه السائب (**Generic Routing Encapsulation** أو **GRE**). يتضمن **GRE** معلومات عن نوع الرزمة التي يتم تغليفها وعن الاتصال بين العميل ووحدة الخدمة. يعتمد الفرق علي مستوي الأمان المطلوب للاتصال، **IPSec** هو الأكثر أماناً و **GRE** له وظيفة أكبر. يستطيع **IPSec** أن يضع رزم **IP** في نفق ويشفرها، بينما يستطيع **GRE** أن يضع رزم **IP** ورزم غير **IP** في النفق. عندما تحتاج إلي إرسال رزم غير **IP** (كـــ **IPX**) عبر النفق، يجب استعمال **IPSec** و **GRE** معاً.

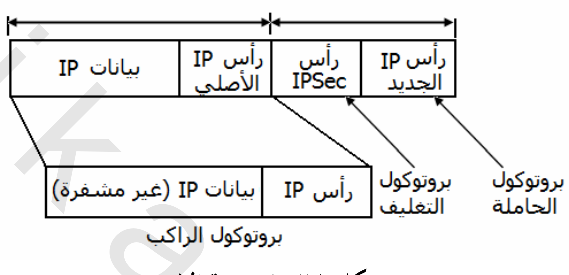
صيغ التشفير

لـــــ **IPSec** صيغتي تشفير : النفق (**Tunnel**) والإرسال (**Transport**). تختلف كل صيغة في طريقة تطبيقها وفي كمية العبء المضاف إلي رزمة البيانات الأصلية التي سيتم تشفيرها في شبكة **VPN** . سنلخّص صيغ العمل المختلفة هذه بإيجاز في أن النفق يشفر رأس الرزمة والحمولة لكل رزمة، بينما الإرسال يشفر الحمولة فقط.

صيغة النفق Tunneling

هذه هي الطريقة العادية التي يتم بها تطبيق **IPSec** بين جداري نار **PIX** (أو عّبارات أمان أخري) متصلين عبر شبكة غير موثوق بها، كالانترنت العمومية. كل المناقشات التي

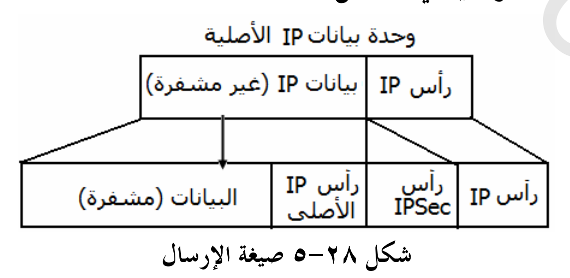
تستخدم **IPSec** ستكون علي صيغة النفق. صيغة النفق تغلف وتحمي رزمة **IP** كاملة. لأنها تغلف أو تخفي الرزم لكي يتم تمريرها بنجاح فإن موجهات التشفير نفسها تملك العناوين **IP** المستعملة في تلك الرؤوس الجديدة. يمكن استخدام صيغة النفق مع بروتوكول **ESP** أو بروتوكول **AH** أو مع كليهما (ستتعرف علي هذين البروتوكولين بعد قليل). يؤدي استعمال صيغة النفق إلي توسيع إضافي للرزمة بحوالي **20** بايت في رأس **IP**، يجب إضافة رأس **IP** جديد للرزمة مع رأس **IP** الجديد، كما هو مبين في الشكل ٢٨–٤.



شكل ٢٨–٤ صيغة النفق

صيغة الإرسال Transport

في صيغة الإرسال يتم تشفير الحمولة فقط وليس رزمة البيانات بأكملها. في صيغة النفق، يشفر **IPSec** الرزمة بأكملها ويكتب رأس **IP** جديداً في الرزمة، مما يحجب معلومات المصدر والوجهة الأصلية. صيغة النفق الأكثر أمناً بشكل متأصل من صيغة الإرسال (بسبب حقيقة أنه يتم تشفير الرزمة الأصلية بأكملها، وليس فقط الحمولة مثلما يحصل في صيغة الإرسال)، كما هو مبين في الشكل ٢٨–٥.



شكل ٢٨–٥ صيغة الإرسال

بروتوكولات IPSec

يستعمل **IPSec** ثلاثة بروتوكولات متممة تشكل عند استعمالها سوية هيكلاً متماسكاً وآمناً يرتكز علي معايير قياسية وملائماً مثالياً للشبكات **VPN**. البروتوكولات الثلاثة المشروحة في معايير **IPSec** القياسية هي :

- **Encapsulated Security Protocol** (أو **ESP**، بروتوكول الأمان المغلف) : يزود سرية وحماية البيانات مع تحقق اختياري للصحة وخدمات اكتشاف التكرار. يغلف **ESP** بيانات المستخدم كلياً. يمكن استعمال **ESP** إما لوحده أو إلي جانب **AH** .
- **Authentication Header** (أو **AH**، رأس التحقق من الصحة) : يزود تحققاً من الصحة وخدمات محاربة التكرار (اختياري). يزود **AH** خدمات لأجزاء محدودة من رأس **IP** والرأس الممدد، مضمَّن في البيانات المطلوب حمايتها (وحدة بيانات **IP** كاملة، مثلاً). يمكن استعمال **AH** إما لوحده أو مع **Encryption Service Payload** (أو **ESP**، حمولة خدمة التشفير) لقد حل **ESP** محل هذا البروتوكول إلي حد كبير ويعتبر استعماله مستنكراً.
- **Internet Security Association Key Management Protocol** (أو **ISAKMP**) "بروتوكول إدارة مفتاح اقتران أمان الانترنت" : يصف مرحلة التفاوض علي اتصال **IPSec** لإنشاء الشبكة **VPN**، يعرف البروتوكول **Oakley** طريقة إنشاء تبادل مفتاح تم التحقق من صحته.

ملخص الفصل

ناقش هذا الفصل استعمال الشبكات **VPN** ، كيف تعمل ، وما هي الفوائد التي تقدمها للشبكات في كل مكان التشفير الذي يزوده **IPSec**، وكيف تستطيع تلك التقنيات أن تضمن المحافظة علي أمان شبكتك وفي الوقت نفسه زيادة الخدمات المتوفرة لعملائك.

تدريبات

١. ما هي الأنواع الثلاثة لشبكات VPN؟

٢. أذكر ثلاثة مزايا لشبكة VPN؟

٣. ما هو الدور الذي يلعبه التحقق من الصحة في حماية تدفق البيانات؟

٤. في الشبكات VPN ما هي صيغتي التشفير ؟

٥. صح أم خطأ.

أ. الهدف من شبكة VPN هو الاتصال بالانترنت

ب. تسمح شبكات VPN بالاتصال عن بعد بالشبكة الرئيسية بأسلوب آمن وموثوق به .

ج. تتسم شبكة VPN بقابليتها للنمو بسهولة أكثر من الخطوط المؤجرة .

٦. متي يحصل شق الأنفاق المنقسم Split Tunneling ؟



الملاحق

الملحق الأول : بطاقات مرجعية

الملحق الثاني : إجابات تمارين الفصول

الملحق الثالث : معجم المصطلحات

الملحق الأول : بطاقات مرجعية

البطاقة الأولي : ملخص مواصفات تقنية الشبكة المحلية

التقنية	أقصى سرعة (ميجا بت /ثانية)	نوع الكابلات	أقصى عدد للوحدات الفرعية للشبكة	أقصى عدد للوحدات الفرعية / القطع
Ethernet				
10 Base5	١٠	كبل محوري سميك	٣٠٠	١٠٠
10 Base 2	١٠	كبل محوري رفيع	٩٠	٣٠
10 Base T	١٠	UTP- 3	١,٠٢٤	٢
10 Base F	١٠	ألياف بصرية		٢
100 Base T	١٠٠	UTP-CAT5	١,٠٢٤	٢
100 Base F	١٠٠	ألياف بصرية		٢
1000 Base T	١٠٠٠	UTP-CAT5		٢
1000 Base F	١٠٠٠	ألياف بصرية		٢
Token Ring Type1	١٦	UTP-CAT5 أو STP		٢٦٠
Type3	٤	UTP-CAT3		٧٢
Fiber	١٦	ألياف بصرية		
FDDI Fiber	١٠٠	ألياف بصرية	٥٠٠	

البطاقة الثانية : قواعد استخدام الكابلات Twisted-Pair

- أقصى امتداد للكابل: 100 متر (330 قدم)
- تتصل جميع أجهزة الكمبيوتر بجهاز hub رئيسي
- يلزم استخدام عنصري مقاوم طرفي عند طرفي الكابل
- كيفية ربط موصل RJ-45 بالكابل

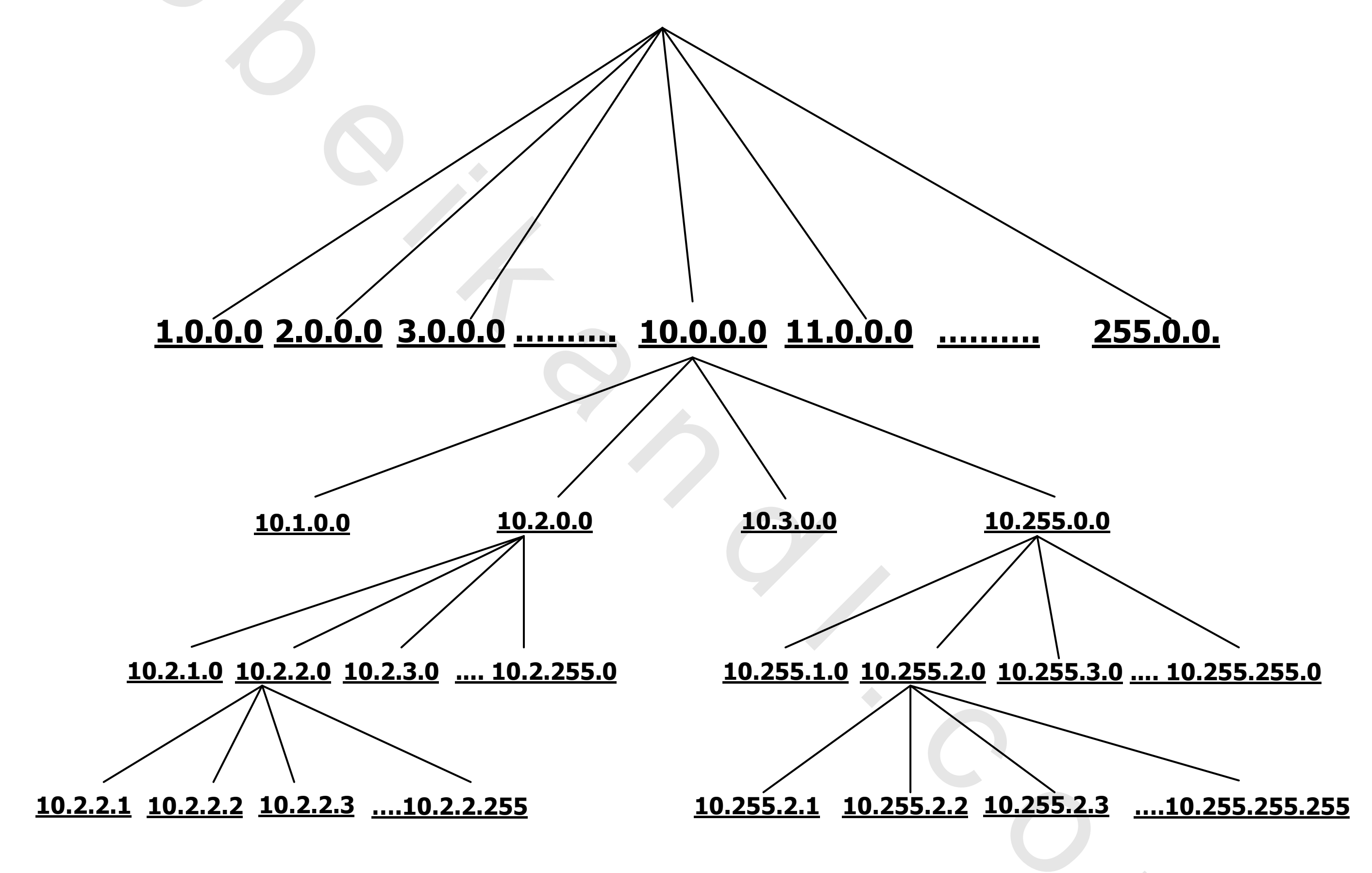
الإبرة Pin	لون السلك
١	أبيض وبرتقالى
٢	برتقالى
٣	أبيض وأخضر
٤	أزرق
٥	أبيض وأزرق
٦	أخضر
٧	أبيض وبنى
٨	بنى

مدى عناوين IP

- Class A : من 10.0.0.0 إلى 10.255.255.255
- Class B : من 172.31.255.255
- Class C : من 192.168.0.0.0 إلى 192.168.255.255

نصائح مفيدة للاحتفاظ بكفاءة الشبكة

- إنشاء نسخ احتياطية بصورة منتظمة
- تسجيل تخطيط الشبكة وتحديثه باستمرار
- الاحتفاظ بكم مناسب من المكونات والأدوات الاحتياطية
- تجنب إغلاق أو إعادة تشغيل وحدة الخدمة أثناء اتصال المستخدمين بها.


Internet Addresses
1.0.0.0
2.0.0.0
3.0.0.0
....
10.0.0.0
11.0.0.0
....
255.0.0.
10.1.0.0
10.2.0.0
10.3.0.0
10.255.0.0
10.2.1.0
10.2.2.0
10.2.3.0
.... 10.2.255.0
10.255.1.0
10.255.2.0
10.255.3.0
.... 10.255.255.0
10.2.2.1
10.2.2.2
10.2.2.3
....10.2.2.255
10.255.2.1
10.255.2.2
10.255.2.3
....10.255.255.255

الملحق الثاني : إجابات تدريبات الفصول

رقم السؤال	الإجابة
الفصل الأول ١	ب
٢	ب ، ج
٣	ب ، ج
٤	وحدة الخدمة ــ بطاقة الشبكة ــ وحدة التوصيل ــ الكابلات والأسلاك
٥	Windows Server 2003 - Netware
٦	ب ، ج ، د
الفصل الثاني ١	فتحات التوسعة
٢	ب ، ج ، أ
٣	أ ، د
٤	د
٥	أ. متغيرة ب. أسرع ج. برامج نظم التشغيل د. بطاقة الشبكة
٦	برامج معالجة النصوص ــ برامج الجداول الحسابية ــ برامج قواعد البيانات ــ برامج الرسم
٧	د
الفصل الثالث ١	55
٢	110001
٣	7B9C

٤	2960
٥	010110101111
٦	F93C
٧	بايت ــ كيلو بايت ــ ميجا بايت ــ جيجا بايت
٨	٤٠٤ دقيقة
٩	هــ
الفصل الرابع ١	ب ، د ، هــ
٢	أ مع ٣ ــ ب مع ٢ ــ ج مع ١
٣	تقع شبكات LAN في منطقة جغرافية واحدة، أما شبكات WAN فإنها عبارة عن مجموعات شبكات محلية موجودة فى أماكن متباعدة ومتصلة ببعضها
٤	الشبكة النظيرة ــ شبكة الوحدة التابعة / وحدة الخدمة
٥	أ خطأ ــ ب خطأ ــ ج صواب ــ د خطأ ــ هــ صواب
الفصل الخامس ١	أ مع ٥ – ب مع ١ – ج مع ٢ – د مع ٣ – هــ مع ٤
٢	أ مع ٢ ــ ب مع ٤ ــ ج مع ٦ ــ د مع ٣ ــ هــ مع ٧ ــ و مع ٥ ــ ز مع ١
٣	هــ
الفصل السادس ١	٢
٢	المادية ــ ربط البيانات ــ الشبكة ــ النقل ــ الجلسة ــ تقديم ــ التطبيق
٣	أ مع ٣ ــ ب مع ٥ ــ جــ مع ٢ ــ د مع ٦ ــ هــ مع ٧ ــ ز مع ٤ ــ و مع ١
٤	د
٥	ج

الفصل السابع ١	هـ
٢	ب
٣	أ – التطبيق ب – الانترنت ج – النقل د –التطبيق هـ – الانترنت و– النقل
٤	ج
٥	أ مع٢ – ب مع ١ – جـ مع ٤ – د مع ٣
الفصل الثامن ١	أ ، ج
٢	أ مع ٤– ب مع ٣ – ج مع ١ – د مع ٢
٣	أ ـــ يزيد عدد التصادمات / ب ـــ شبكة جامعة / ج ـــ وحدة التوصيل / د ـــ لا تدعم / هـــ ـــ لأن سرعة نقل البيانات فى الجهاز أكبر من سرعة نقل البيانات على كابل الشبكة
٤	نوع البطاقة ـــ نوع الناقل الذي تستخدمه البطاقة ـــ الماركة أو الشركة المصنعة للبطاقة
٥	تحتوي المنافذ العادية على دوائر عبور، أما المنفذ التوسعي فلا يحتوي على دوائر عبور
٦	ج
٧	ج
٨	أ خطأ ـــ ب صواب ـــ ج صواب ـــ د خطأ
٩	أ
١٠	ألياف أحادية النمط ـــ الألياف متعددة الأنماط
الفصل التاسع	
١	هـ
٢	ب
٣	وحدة خدمة مستقلة للملفات – وحدة خدمة مستقلة للطابعات

	– وحدة خدمة مستقلة لمشغلات الأقراص.
٤	أ– خطأ ب– صواب جـ – صواب
٥	ب
الفصل العاشر	
١	ب جـ أ د
٢	١ مع د ، ٢ مع جـ ، ٣ مع ب ، ٤ مع هـ ، ٥ مع أ
الفصل الحادي عشر	
١	– اختيار تخطيط الشبكة – اختيار نظام تشغيل الشبكة – تحديد الغرض من إنشاء الشبكة .
٢	د
الفصل الثاني عشر	
١	– أغلق جهاز الكمبيوتر قبل القيام بأي توصيلات أو تثبيت أحد مكونات الشبكة. استخدم الأدوات المناسبة. ضع علامات علي الكابلات والوصلات التي تقوم بفكها لتميزها ليسهل عليك إعادة تجميع الكمبيوتر بعد فكه.
٢	د
الفصل الثالث عشر	
١	أ– خطأ ب– صواب ج– خطأ د– صواب

٢	١ مع ب ، ٢ مع د ، ٣ مع أ ، ٤ مع جـ
الفصل الرابع عشر	
١	تمرين عملي
الفصل الخامس عشر	
١	تمرين عملي
الفصل السادس عشر	
١	تمرين عملي
الفصل السابع عشر	
١	عنوان IP هو الذي يتيح لكل جهاز موجود علي الشبكة أن يتعرف علي باقي الأجهزة ، ويعمل عند الطبقة الثالثة من نموذج OSI وهي طبقة الشبكة (Network Layer) أما عنوان MAC فهو العنوان المادي الذي يتم تعيينه لكل جهاز موجود علي الشبكة، وهو عادة العنوان المخصص لبطاقة الشبكة، ويعمل عند الطبقة الثانية من نموذج OSI وهي طبقة Data Link .
٢	أ – IPv4 ب – IPv6 ج – IPv4 د – IPv6 هـ – IPv6 و– IPv4
٣	ج
٤	ج
٥	العناوين الخاصة
٦	2^{24}-2 = 16777214
٧	من 128.0.0.0 إلي 191.255.0.0
٨	أ – خطأ ب – صواب ج – خطأ د – صواب هـ – صواب
٩	أ – وحدة الخدمة والطابعات ب – DHCP
١٠	ب

الفصل الثامن عشر	
١	ج
٢	ب
٣	عنوان الجهة المستقبلة لحزمة البيانات الواردة
٤	د
٥	أ– المحول ب – الموجه ج – المحول د – الموجه هـ – المحول و – الموجه ز – الموجه
٦	جـ
٧	يولد رسالة خطأ
٨	ROUTE PRINT
٩	ROUTE ADD
١٠	ب
الفصل التاسع عشر	
١	العناوين الخاصة
٢	أ ، ج
٣	أ – تؤدي إلي 175.12.24.0 ب – تؤدي إلي 194.17.197.208
٤	جـ
٥	جـ
٦	أ – ٦٢ ب – ٢ جـ – الشبكة الأولي : 192.212.31.4 الشبكة الثانية : 192.21231.8 الشبكة الثالثة : 192.212.31.12 الشبكة الثانية والستين : 192.212.31.248 د – الشبكة الأولي 195.212.31.5 و 195.212.31.6 الشبكة الثانية : 195.212.31.9 و 195.212.31.10

	الشبكة الثالثة : **195.212.31.13** و **195.212.31.14** الشبكة الثانية والستين : **195.212.31.249** و **195.212.31.250** هـ – عنوان بث الشبكة الأولي : **195.212.31.7** عنوان بث الشبكة الثانية : **195.212.31.11** عنوان بث الشبكة الثالثة : **195.212.31.15** عنوان بث الشبكة الثانية والستون : **195.212.31.251**
٧	لا. لأن **195.212.31.5** موجود علي الشبكة الأولي و **195.212.31.9** موجود علي الشبكة الثانية
الفصل العشرون	
١	– **يجب أن يتسم مدير الشبكة بالنظام واليقظة وأن يكون دقيقا فى عمله.** – **يتأكد من تطبيق الإجراءات السليمة لمقاومة الفيروسات على كل جهاز.** – **يقوم بإجراء النسخ الاحتياطي في مواعيده .**
٢	أ– صواب ب – صواب جـ – خطأ د – خطأ
٣	– متابعة حالة الأجهزة والكابلات وكروت الشبكة وأجهزة التوصيل (**Hub**) أو أجهزة التبديل (**Switch**) وغيرها من الأجهزة ، بالإضافة إلى نظام التشغيل . – العمل على تطوير الشبكة باستمرار بأحدث الأجهزة. – تثبيت برامج الكشف علي الفيروسات وتثبيت جدار النار لتأمين الشبكة من الفيروسات والقرصنة.
الفصل الحادي والعشرون	
١	– النسخ الاحتياطي التام أو الكلي **Full Backup**. – النسخ الاحتياطي المتباين **Differential Backup**.

	– النسخ الاحتياطي التزايدي **Incremental Backup**.
٢	أ– صواب ب– خطأ جـ – صواب د– صواب
الفصل الثاني والعشرون	
١	– أفحص الكابلات والتأكد من سلامة توصيلها. – أتأكد من توصيل الجهاز بمصدر الطاقة أو مثبت التيار. – أتأكد من توصيل الشاشة بمصدر الطاقة جيداً.
٢	أ. مراقبة أداء المعالج. ب. مراقبة أداء محرك القرص. ج. مراقبة أداء الذاكرة.
الفصل الثالث والعشرون	
١	يعمل نظام حسابات المستخدمين وكلمات المرور علي قصر حق الدخول إلي الشبكة علي المستخدمين المصرح لهم فقط بذلك.
٢	– استخدم نظم تأمينية – استخدم نظام IPSec للمساعدة علي الحماية ضد الهاكرز الذي يحاولون التلصص علي اتصالات الشبكة من الشبكة الداخلية. – استخدم برامج الحماية من الفيروسات.
الفصل الرابع والعشرون	
١	– تأكد من وجود برنامج للكشف عن الفيروسات علي الجهاز الذي تستخدمه. – لا ترسل المعلومات السرية والهامة مثل كلمات المرور وأرقام بطاقة ائتمان عبر الانترنت. – لا تفتح ملفات أو بريد مجهول المصدر أو يحتوي علي عنوان مريب. – لا تسمح لأي جهاز متصل بالانترنت بتنشيط مشاركة

	الملفات لاتصالات TCP/IP .
٢	– أفرض نظاماً صارماً علي كلمات المرور وتأكد من أنها تستخدم بسرية تامة. – أحتفظ بوسائط النسخ الاحتياطي في مكان آمن بعيداً عن أجهزة الشبكة. – أتأكد تماماً من أن برامج مضادات الفيروسات كافية.
الفصل الخامس والعشرون	
١	نعم
٢	يحتاج لجدار النار كل شخص متصل بالانترنت، أو لديه موارد تكنولوجيا المعلومات ويريد حمايتها.
٣	لأنه يزود حماية لشبكتك من خلال تقنيات كـ SPI التي لا تكون ممكنة مع أي جهاز آخر.
٤	قواعد جدار النار تطابق أسلوب أمان الشبكة في مؤسستك كما هو مذكور في أسلوب الأمان المكتوب.
الفصل السادس والعشرون	
١	يقال عن شبكة أنها شبكة WAN إذا كانت تلبي الشروط الآتية : – تتصل بشبكات خاصة. – ترسل البيانات عبر خطوط الهاتف – يمكن توثيق المستخدمين علي الطرفين
٢	– خطوط اتصال هاتفي قياسية – خطوط هاتفية رقمية
٣	– خطأ ب– صواب جـ– صواب

الفصل السابع والعشرون	
١	الحوائط – الأحوال الجوية السيئة – تداخل الإشارات اللاسلكية – عدم ضبط الجهاز المعدني (Antenna) الذي يرسل ويستقبل الإشارات
٢	أ – خطأ ب – صواب جـ– خطأ د– صواب
٣	١. رخص السعر ٢.حرية الحركة ٣. سهولة تمديد الشبكة
٤	يشرح هذين المصطلحين المعيار القياسي اللاسلكي من مؤسسة IEEE ، وهي تستعمل بشكل متبادل. Wi-Fi هي الكلمة الشائعة المقترنة بالمعيار القياسي 802.11 .
٥	Ethernet
٦	أ– خطأ ب – صواب جـ – صواب
الفصل الثامن والعشرون	
١	بين المواقع – الاكسترانت – الاتصال عن بعد
٢	–آمنة – تشفير البيانات أثناء مرورها – يمكن استعمالها لربط المواقع بأمان عبر الانترنت.
٣	يرسخ التحقق من الصحة وسلامة تدفق البيانات ويضمن أنه لم يتم العبث به عند عبوره.
٤	أ– صيغة النفق ب – صيغة الإرسال
٥	أ– خطأ ب– صواب ج– صواب
٦	يحدث شق الأنفاق المنقسم عندما يسمح لمستخدم أو موقع VPN بعيد بالوصول إلي شبكة عمومية (الانترنت) في نفس الوقت الذي تتصل فيه بشبكة VPN الخصوصية من دون وضع بيانات الشبكة العمومية داخل النفق أولاً.

قاموس المصطلحات

مع تغير المصطلحات التقنية الخاصة بالكمبيوتر عموماً وبربط الشبكات بـصفة خاصـة ، تتغير أيضا قواميس المصطلحات . لا يتعرض قاموس المصطلحات هنا لكل شـيء. علـى الرغم من ذلك، هناك قواميس مصطلحات على الويب التي تقدم تعريفات لمـصطلحات الكمبيوتر وربط الشبكات الحالية. إذا كنت ترغب في التعرف علي المزيد من المصطلحات أو إذا لم تجد المصطلح الذي تبحث عنه في هذا الملحق، اذهب إلي أحد مواقع الويب التي تقدم تعريفات لمصطلحات الكمبيوتر وربط الشبكات ويتم تحديثها بصفة متكررة. ومنها علي سبيل المثال **WWW.Webopedia.Com.** .

لقد قمت بترتيب المصطلحات في هذا الملحق طبقاً للترتيب الأبجدي للحروف الانجليزيـة نظراً لسهولة الوصول إليها. لأن هذا هو الأصل الذي نحاول فهمه.

10BASE-2 : شبكة Ethernet تعمل على كبل محورى من نوع RG58. تـــدعم 10BASE-2 ، التي يطلق عليها أيضا Thinnet أو الشبكة الأقل تكلفة ، مقاطع شبكة يصل طولها إلي 185 مترا. يعد ذلك تخطيط أداة نقل ولا يمكن أن يقاوم أية مقاطعات فى أى كبل بين جهازى كمبيوتر. الرقم " 10" يشير لسرعة الشبكة وهى 10 Mbps، الكلمة "base" تشير إلى أن الشبكة تستخدم نطاقا أساسيا للإرسال و الـــرقم "2" يشير إلى أقصى طول لقطع الكبلات وهو 200 مترا (١٨٥ متراً بالتحديد) .

10BASE-5: يشبه 10BASE-5، الذى يطلق عليه أيضا Ethernet الكبل الأصـــفر، 10BASE-2 ولكنه يستخدم كبل أكثر سمكا ولذلك تعرف أيضاً باسم Thick Ethernet أو Thicknet. لكل جهاز كمبيوتر مرفق بمقطع 10BASE-5 جهاز يطلق عليه المرسل المستقل (يعرف أيضا باسم Vampire Tap) الذى يصل جهاز الكمبيوتر بأسلاك الشبكة . يعد 10BASE-5 تخطيط أداة نقل ، ولا يمكـــن أن يقـــاوم انقطاع اتصال أى من أجهزة الكمبيوتر . الرقم "10" يشير لسرعة الشبكة وهى 10 Mbps ، الكلمـــة " base" تشير إلى أن الشبكة تستخدم نطاقا أساسيا للإرسال والرقم "5" يشير إلى أقصى طول لقطع الكبلات وهو 500 مترا.

10BaseF: المصطلح الذى يجمع المواصفات الثلاث للطبقة الفيزيائية فى شبكات Ethernet التي تعمـــل بسرعة 10 Mbps وتستخدم الليف الضوئي . يصل أقصي طول لقطع الكابلات إلي ٢,٥ ميـــل (٤٠٢٣٤ متر تقريباً) .

10BaseT: اختصار لأحد المقاييس الثلاثة للطبقة الفيزيائية فى شبكات Ethernet التي تستخدم كبلات UTP فى بنية نجمية. الرقم " 10" يشير لسرعة الشبكة وهى 10 Mbps ،الكلمة "base " تـــشير إلى أن الشبكة تستخدم نطاقا أساسيا للإرسال، والحرف "T " يشير لاستخدام كبلات UTP Cat3 . وأقـــصى طول لقطع الكبلات فى هذه الشبكة هو100 متر . نظرا لأن 10BASE-Tيعد تخطيط نجمى ، فإنه أكثر قوة من 10BASE-2 أو 10BASE-5ويسهل كثيرا من قطع اتصال أجهزة الكمبيـــوتر بالـــشبكة . (دون مقاطعة الشبكة)

100BaseT : اختصار لأحد المقاييس الثلاثة للطبقة الفيزيائية فى شبكات Ethernet التي تعمل بـــسرعة 100 Mbpsوالمعروفة أكثر باسم Fast Ethernet. تستخدم كبل UTP من الفئـــة Category5 فى بنية نجمية بطول أقصى لقطع الكبلات هو 20 متر .

100BaseF : اختصار لمواصفة الطبقة الفيزيائية في شبكات Ethernet التي تستخدم الألياف الـــضوئية. بطول أقصي لقطع الكبلات هو ١٣٥١ قدماً (٤١١,٨ متر تقريباً).

1000 Base T : اختصار لمواصفة الطبقة الفيزيائية فى شبكات Gigabit Ethernet التى تعمل بسرعة 1.000 Mbps تستخدم كبل UTP من الفئة Category 5 أو 5E.

1000Base F: اختصار لمواصفة الطبقة الفيزيائية فى شبكات Gigabit Ethernet التى تعمل بسرعة 1.000 Mbps . تعمل على كبل ليف بصرى بطول أقصي لقطع الكبلات هو ١٨٠٠ قدماً (٥٤٨,٦٤ متراً تقريباً) .

100Base FX: اختصار لأحد المقاييس الثلاثة للطبقة الفيزيائية فى شبكاتFast Ethernet التى تعمل بسرعة Mbps 100 تستخدم الليف البصري فى بنية نجمية. نظراً لأن الألياف الضوئية يمكن أن تحمل البيانات إلي مسافة أبعد مما تحمله الأسلاك النحاسية، فإنها لها أطوال كابلات أعلي بكثير من 100Base-T.

100Base FL : انظر 100Base FX .

56K: خط هاتف رقمى يمكن أن يحمل البيانات بسرعات تصل إلي 56 كيلوبت فى الثانية.

802.3 : معيار أنشأه معهد المهندسين الكهربائين والإلكترونين المعروف بـ IEEE المعروف بصورة عامة باسم Ethernet.

802.11 : معيار IEEE للشبكات اللاسلكية. ينقسم هذا المعيار إلى 802.11a. و 802.11b و 802.11g .

802.11b : عائلة مواصفات أنشأها معهد المهندسين الكهربائين والإلكترونين (IEEE) لشبكات الايثرنت اللاسلكية في مساحة عرض نطاق البث 2.4 جيجاهرتز. ويقدم سرعات اتصال تصل إلي ١١ ميجابت في الثانية.

802.11g : معيار قياسي لاسلكي جديد من IEEE مرتفع السرعة يتيح للمستخدمين إرسال البيانات بسرعة تصل إلي 54 ميجابت بالثانية – تقريباً خمس مرات أسرع من التقنية 802.11b .

Access Point (**نقطة وصول**): هو جهاز يوفر اتصال بين وحدة تابعة لاسلكية وباقي الشبكة. تعمل نقطة الوصول بصفتها موصل طبقة 2 الذى يوفر الاتصال بين الشبكات السلكية واللاسلكية .

Adapter card (**بطاقة محول**) : ينطبق هذا التعريف بصفة أساسية على أجهزة الكمبيوتر المتوافقة مع Intel. تعد بطاقة المحول تجميعا إلكترونيا يتصل بجهاز كمبيوتر من خلال واجهة استخدام قياسية (انظر card- slot interface (واجهة فتحة بطاقة) لاحقا فى قاموس المصطلحات) يطلق عليه فتحة بطاقة . يمكن أن توفر بطاقات المحولات مجموعة متنوعة من الخدمات لجهاز الكمبيوتر، ومنها وظائف الفيديو والشبكة

والمودم وغيرها من الوظائف.

Administration (**الإدارة**) : هى مهمة تهتم في الأساس بالحفاظ على الشبكة عاملة بصفة مستمرة دون مشكلات. تم تخصيص الجزاء الخامس من هذا الكتاب لهذا الموضوع .

Analog phone line (**خط هاتف قياسى**) : خط هاتف يرسل الصوت بصفته شكل موجة (مثل: موجة المذياع). تعد خطوط الهاتف القياسية شائعة ؛ ومن المحتمل أن تكون خطوط الهاتف القياسية هى الخطوط الموصل بها هاتفك المنزلى. لإرسال بيانات عبر خط هاتف قياسى ، يجب عليك تحويله من بيانات رقمية إلي صوت.

Application layer (**طبقة التطبيق**) : أعلى طبقة فى نموذج OSI المرجعى ، تقدم مدخلا تستخدمه التطبيقات للوصول إلى كافة بروتوكولات الشبكة .

ASCII: اختصار لعبارة American Standard Code for Information Interchange (الرموز القياسية الأمريكية لتبادل المعلومات) ، وهى طريقة تترجم بها أجهزة الكمبيوتر بتات 1 و 0 (رموز ثنائية يمكن لأجهزة الكمبيوتر فهمها) إلي أحرف أبجدية وأرقام ؛ وغيرها من الأحرف التى يمكن للبشر فهمها.

ATM: اختصار لعبارة Asynchronous Transfer Mode (وضع النقل غير المتزامن)، وهو تخطيط جديد لإرسال البيانات عبر شبكة . يعد ATM معقدا ، ولكنه له العديد من المزايا مقارنة بالتخطيطات القديمة، مثل : Ethernet و Token Ring. نادرا ما يتم استخدام ATM على الشبكات الصغيرة ، نظرا لتكلفته الباهظة ؛ ولكنه يتم استخدامه بصفة شائعة فى شبكات WAN الكبيرة .

Attenuation (**التلاشي**): الانخفاض المتزايد للإشارة أثناء عبورها كبل أو وسيط آخر.

Authentication (**التحقق من الصحة**) : هى عملية التأكد بقدر الإمكان من أن عمليات تسجيل الدخول والرسائل الواردة من مستخدم معين (مثل: كلمة مرور أو بريد إلكتروني) تأتى من مصدر مصرح به.

Authentication Header أو **AH** (**رأس التحقق من الصحة**) : يزود تحققاً من الصحة وخدمات محاربة التكرار (اختياري). يزود AH خدمات لأجزاء محدودة من رأس IP والرأس الممدد لكنه لا يهتم بتشفير البيانات بتطبيق بعثرة أحادية الاتجاه لإنشاء رسالة تلخيصية للرزمة.

Backup (**نسخة احتياطية**): نسخة من الملفات المهمة يتم الاحتفاظ بها تحسبا لأى ضرر قد يقع بالملفات الأصلية. يتم إنشاء هذه النسخة الاحتياطية يوميا أو أسبوعياً أو علي فترات دورية يحددها المسئول عن ذلك.

Bandwidth (**تردد نطاق**): قياس قدر البيانات التي يمكن لوسط معين حملها. على سبيل المثال: يبلغ تردد النطاق لخط الهاتف المتوسط نحو 33.6 كيلوبت في الثانية فقط، بينما يبلغ تردد النطاق لخط هاتف رقمى TI نحو 1.544 ميجابت في الثانية.

Binary (**ثنائى**): نظام حسابي يستخدمه الكمبيوتر. يستخدم هذا النظام الأساس 2 بدلاً من الأساس 10 في النظام العشري المألوف لنا. وهو يعبر عن وجود حالتين فقط ويستخدم رمزين فقط هما 0 و 1. في الرموز الثنائية، يتم تمثيل 1 بالثنائي 1 و 2 بالثنائي 10 و 3 بالثنائي 11 و 4 بالثنائي 100 و 5 بالثنائي 101 ... وهكذا.

Bit (**بت**): جزء من المعلومات يتم تمثيله بصفته 1 أو 0 بالنسبة لجهاز الكمبيوتر.

BNC: اختصار للعبارة Bayonet- Neill- Councilman وهو نوع من وصلات الكبلات المستخدمة على شبكات Thin Ethernet.

Bridge (**جسر**): جهاز ربط فى الشبكات يعمل على طبقة ربط البيانات فى نموذج OSI المرجعى (الطبقة رقم ٢) ويصفى إشارات الشبكة بحسب وجهة الرزم.

Broadcast (**بث أو بلاغ**) : رسالة تعمم على كل الكمبيوترات على الشبكة المحلية. تستخدم بروتوكولات طبقة ربط البيانات عناوين خاصة معينة كعناوين بث، مما يعنى أن كل الكمبيوترات التى تتلقى الرسالة تقرؤها فى الذاكرة وتعالجها. تستخدم الشبكات المحلية البلاغات (البث) لعدد من المهام، مثل البحث عن معلومات تتعلق بكمبيوترات أخرى على الشبكة.

Browser (**برنامج استعراض**) : هو برنامج يوفر طريقة لعرض المستندات المتوفرة على شبكة الويب العالمية وقراءتها. يعد كل من Microsoft Internet Explorer, Netscape Navigator برنامج استعراض.

Bus topology (**تخطيط أداة نقل**): هو تخطيط شبكة حيث تتصل كل أجهزة الكمبيوتر بصورة متسلسلة بطول الكبل. لا يمكن الاعتماد على شبكات أداة النقل . فإذا تلف أحد مقاطع الكبل ، سوف تفشل الشبكة بأكملها . تعد 10BASE-2 و10BASE-5 أمثلة على شبكات أداة النقل .

Byte (**بايت**): هى ثماني بتات (يطلق عليها أيضا ثماني (أو Octet) عند مناقشة TCP/IP). يساوى البايت حرفا واحدا. ويمكن أن يمثل البايت (ثماني بتات) 256 رقما (من 0 إلي 255) فى الأرقام الثنائية.

Cable modem (**كبل مودم**): هو جهاز يتم استخدامه بواسطة مزودى الكبلات لتوفير بيانات عالية

السرعة باستخدام الكبل بصفته الوسط.

cache (**ذاكرة وسيطة**) : أحد الأشكال المعقدة لتخصيص مساحة تخزين مؤقتة للبيانات التي يتم فيها تخصيص كم كبير من الذاكرة للاحتفاظ بالبيانات لسهولة الوصول إليها .

Card- slot interface (**واجهة فتح بطاقة**): هى مكان يتم فيه تركيب بطاقات المحولات فى أجهزة الكمبيوتر الشخصية المتوافقة مع Intel. تأتى واجهات فتحات البطاقات فى عدة أشكال : ISAوVESA و EISA (أصبحت كلها قديمة الآن) وPCI.

Cat3: التصنيف Category 3 لكبلات UTP الذى كان فى أحد الأيام أكثر الوسائط استخداماً لشبكات الهاتف والبيانات .

Cat5: التصنيف Category 5e أو Enhanced Category 5 (الفئة 5 المحسنة) وهو تصنيف جديد نسبيا لكبلات UTP مصمم لشبكات البيانات التى تعمل بسرعة عالية جدا"، مثل شبكات Gigabit Ethernet.

Category n: اصطلاح يستخدم لتعيين تصنيف لكبلات UTP ، بالاعتماد على المعايير التى تضعها EIA/TIA.

CDPD : اختصار لعبارة Cellular Digital Packet Data (بيانات الحزمة الرقمية الخلوية) ، وهى أكثر الطرق شيوعا لإرسال البيانات عبر الارتباطات اللاسلكية. تستخدم CDPD تردد مذياع يبلغ 2.4 جيجاهرتز.

Client (**وحدة تابعة**): جهاز كمبيوتر يستخدم الموارد التى تشاركها أجهزة كمبيوتر الخادمات.

Clint/server model (**نموذج وحدة تابعة / وحدة خدمة**): هى شبكة يتم فيها توزيع المعالجة بين جهاز خادم (وحدة خدمة) ووحدة تابعة ، حيث يكون لكل منهما دور محدد. يتم استخدام هذا النموذج أيضا لوصف الشبكات التى لها خادمات مخصصة . هى عكس شبكات نظير بنظير .

Clustering (**تجميع خادمات**): فى ربط الشبكات ، يعد تجميع الخادمات هو طريقة تجميع خادمات متعددة بحيث إذا فشل أحد الخادمات ، يتولى الأمر خادمات أخرى.

Coaxial cable (**كبل محورى**): هو كبل بموصلين به موصل مركزى ثابت وموصل خارجى مضفر. يتم استخدام الكبل المحورى لشبكات 10BASE-2 ويشبه الكبل المستخدم لكبل التلفاز .

Collision (**تصادم**): فيما يتعلق بربط الشبكات ، هو ما يحدث عندما يحاول جهازى كمبيـــوتر إرســـال البيانات على نفس أسلاك الشبكة فى نفس الوقت . يؤدى ذلك إلي إنشاء تعارض ؛ ويشعر جهازا الكمبيوتر بالتعارض ويوقفان الإرسال وينتظران وقتا عشوائيا قبل إعادة الإرسال .

Collision domain (**نطاق التصادم**): مجموعة من الكمبيوترات سيتسبب فيها أى كمبيوتران يرسلان بيانات فى نفس الوقت بحدوث تصادم. كل الكمبيوترات على الشبكة المحلية تقع فى نفس نطاق التـــصادم، فى حين أن الكمبيوترات الموجودة على شبكتى أجزاء يصل بينهما جسر أو موجه تقع فى نطاقي تصادم مخـــتلفين وذلك لأن المعالجة التى يقوم بها الجسر أو الموجه تسبب تأخيرا بسيطا بين توليد الرزمة على أحـــد الجـــزئين ومكاثرتها على الجزء الآخر. لتجنب حدوث تصادم يمكن أن يرسل كل جهاز كمبيوتر البيانـــات عنـــدما لا تكون هناك أجهزة كمبيوتر أخرى ترسل البيانات .

COM1: أول منفذ متسلسل على جهاز الكمبيوتر .

Concentrator (**وحدة تجميع**): يطلق عليها أيضا وحدة تركيز أو MAU. تساعد وحدة التجميع علي التأكد من قوة الشبكة عن طريق التأكد من أنه لا يمكن قطع اتصال الشبكة نظرا لفشل فى كبل واحد .

Configuration management (**إدارة التوصيف**) : هو فن التأكـــد مـــن أن محطـــات عمـــل المستخدمين مثبت عليها الأجهزة والبرامج الصحيحة وأن البرامج والأجهزة قد تم إعدادها وفقا لمقاييس متفق عليها ومسبقة الإعداد .

Connection- oriented (**قائم على الاتصال**) : نوع من البروتوكولات يرسل سلسلة من الرســـائل إلى الجهة بهدف تأسيس اتصال ، قبل إرسال أية بيانات. تأسيس الاتصال يضمن أن النظام الوجهـــة فعـــال وجاهز لاستلام البيانات . تستخدم البرتوكولات القائمة على الاتصال فى العادة لإرسال المقادير الكبيرة مـــن البيانات. كإرسال ملفات كاملة والتى يجب تقطيعها إلى عدة رزم لن تكون ذات فائدة إلا إذا وصلت كلـــها إلى النظام الوجهة بدون أخطاء. البروتوكول TCP بروتوكول قائم على الاتصال.

Connectionless (**عديم الاتصال**): نوع من البروتوكولات يرسل الرسائل إلى الوجهة دون تأســـيس اتصال من البداية مع النظام الوجهة. تسبب البرتوكولات عديمة الاتصال بعض المشاكل وهى تستخدم بشكل رئيسى فى الاجرائيات التى تتألف من رسالتى طلب ورد فقط. البرتوكـــولان IP و UDP كلاهمـــا عـــديم الاتصال.

Cracker (**مخرب**): شخص ينفذ عمليات وصول غير مصرح بها إلي نظم أجهزة كمبيوتر الآخرين . وعادة ما يكون لديه نوايا غير حسنة .

CSMA/CD : اختصار لعبارة Carrier Sense Multiple Access/Collision Detection (الوصول المتعدد لتحسس الحامل / اكتشاف التعارض)، وهو وسيلة تتبادل بها أجهزة الكمبيوتر البيانات فى شبكات Ethernet.

CSU/DSU: اختصار لعبارة Channel Service Unit/Data Service Unit (وحدة خدمة القناة/ وحدة خدمة البيانات) ، وهو جهاز يغير حزم بيانات الشبكة المحلية إلي حزم بيانات يمكن نقلها عبر WAN.

Datagram (**مخطط بيانى**): مصطلح يشير إلى البيانات المستخدمة من قبل البروتوكول IP والبروتوكولات الأخرى العاملة على طبقة الشبكة . تتلقى بروتوكولات طبقة الشبكة البيانات من بروتوكولات طبقة النقل وترزمها فى مخططات بيانية عن طريق إضافة الترويسات الخاصة بها. بعد ذلك يمرر البروتوكول المخططات البيانية للأسفل نحو بروتوكول طبقة ربط البيانات من أجل رزمها أكثر قبل أن يتم إرسالها عبر الشبكة.

Decimal (**عشرى**): طريقة كتابة الأرقام التى نستخدمها طوال الوقت ؛ تستخدم الأساس 10، يتم العد من 1إلى 9 كما يلى : 1و2 و3 و4 و5 و6 و 7و8 و 9 وهو غير الرموز الثنائية والسداسية العشرية.

Default gateway (**بوابة افتراضية**) : يستخدم الموجه الشبكة المحلية من قبل كمبيوتر عميل TCP/IP لإرسال الرسائل إلى كمبيوترات على شبكات أخرى.

Destination Address (**عنوان الجهة**): حقل بطول 48 بت فى ترويسة بروتوكول طبقة ربط البيانات يحتوى على متتالية ست عشرية تستخدم لتحديد واجهة الشبكة التى سيتم إرسال الإطار إليه.

Destination IP Address (**عنوان IP للنظام الجهة**): حقل بطول 32 بت فى ترويسة IP يحتوى على قيمة تستخدم لتحديد وجهة الشبكة التى سيتم إرسال الرزمة إليها.

DHCP: اختصار لعبارة Dynamic Host Configration Protocol (برتوكول توصيف مضيف ديناميكى) ، وهو جزء من مجموعة برتوكولات TCP/IP التى تتعامل مع التعيين التلقائى لعناوين IP للوحدات التابعة.

Differential backup : أحد أنواع النسخ الاحتياطي يتم فيه الاقتصار على نسخ الملفات التى تم تعديلها بعد آخر نسخة احتياطية كاملة تم إنشاؤها .

Digital (**رقمى**): نوع لإرسال البيانات يعتمد على البيانات التى يتم تشفيرها بالنظام الثنائي (أى البيانات التى يتم تنسيقها باستخدام بتات 1و0) .

Digital Phone Line (**خط هاتفى رقمى**) : خط هاتف يحول الصوت إلي بيانات رقمية. تعمل خطوط الهاتف الرقمية مع أجهزة الكمبيوتر بصورة أفضل من خطوط الهاتف القياسية ، لأن أجهزة الكمبيوتر ترسل المعلومات رقميا. يتم غالبا استخدام خطوط الهاتف الرقمية لشبكات WANs، حيث يجب إرسال البيانات بسرعات عالية لمسافات طويلة.

Directory services (**خدمات الدليل**) : مجموعة من الأدوات التى تمكن مديرى الشبكة من تزويد المستخدمين بإمكان وصول إلي موارد محددة مستقلة عن مكان تسجيل دخول المستخدمين على الشبكة. أى إذا كان شخص فى قسم التسويق لديه إمكان وصول إلي الخادمين 2 و1، فإنه لا يمكنه الوصول إلي الخادم 3، بغض النظر عما إذا سجل الدخول إلي الشبكة على جهاز كمبيوتر فى قسم التسويق أو الإنتاج أو الإدارة.

DNS: اختصار لعبارة Domain Name System (نظام أسماء النطاقات) ، وهو جزء من مجموعة. برتوكولات TCP/IP يحلل عناوين IP إلي أسماء . على سبيل المثال : يحلل DNS العنوان 192.168.1.5 إلي CS.library.com.

Domain (**نطاق**) : مجموعة من أجهزة الكمبيوتر التى يتم توثيق تسجيل الدخول عبر الشبكة الخاص بها من خلال خادم Microsoft، علي سبيل لمثال : خادم يستخدم نظام تشغيل الشبكات Windows 2003 Server. يأخذ النطاق عملية التوثيق بعيدا عن محطات العمل الفردية ؛ ويجعلها متمركزة على الخادم .

Domain controller (**وحدة تحكم فى النطاق**): الخادم الذى يوفر توثيق المستخدم ويحافظ على قاعدة بيانات كائنات الشبكة لنطاق Microsoft.

Domain Name System (DNS) (**نظام أسماء النطاقات**): حيز أسماء شجرى موزع متخصص لتقديم أسماء أليفة للكمبيوترات والمستخدمين على شبكات TCP/IP(مثل الانترنت).

DSL: اختصار لعبارة Digital Subscriber Line (خط مشترك رقمى) ،وهو وسيلة توفر بها شبكة الهاتف خدمات بيانات رقمية عالية السرعة عبر أسلاك نحاسية مزدوجة.

Dynamic allocation (**التخصص الديناميكى**) : نمط عملياتي لخادمات DHCP يقوم فيه الخادم بإعطاء عنوان IP ديناميكياً .

Dynamic routing (**التوجيه الديناميكي**): نظام تقوم فيه الموجهات تلقائيا ببناء جداول التوجيه الخاصة بها باستخدام برتوكولات متخصصة للاتصال مع الموجهات المجاورة.

Encapsulation (تغليف): عملية أخذ حزمة بيانات لأحد البروتوكولات ووضع معلومات بروتوكول آخر حولها . يشبه ذلك وضع خطاب فى مظروف وإغلاقه وعنونة المظروف ثم وضع المظروف الأول المغلق فى مظروف ثان معنون بلغة مختلفة. لا تعد هذه طريقة فعالة ، كما أنها تهدر الموارد والوقت . للأسف ، غالبا ما تعد هذه هى الطريقة الوحيدة لتحقيق أمر ما .

Encryption (تشفير) : وسيلة لتحقيق أمان البيانات بترجمتها باستعمال مفتاح (كلمة مرور). يمنع التشفير إمكانية قراءة كلمة المرور أو المفتاح بسهولة في ملف التكوين.

Encryption Key (مفتاح تشفير): سلسلة من الأحرف والأرقام المستخدمة لتحويل رسائل بنص عادى إلي نصوص مشفرة . يعتمد تأمين مفتاح التشفير على طوله .

Error correction (تصحيح الخطأ): عملية التأكد من أن البيانات التي يتم نقلها عبر السلك تتم بصورة صحيحة. عادة ما تعمل عملية تصحيح الخطأ باستخدام مجموعة اختبار لتحديد ما إذا كانت البيانات تلفت أثناء النقل أو لا. تستهلك عملية تصحيح الخطأ قدرا معينا من تردد نطاق أى اتصال .

ESP اختصار للعبارة Encapsulated Security Protocol (بروتوكول الأمان المغلف) : بروتوكول أمان يزود سرية وحماية البيانات مع تحقق اختياري للصحة وخدمات اكتشاف التكرار. يغلف ESP بيانات المستخدم كلياً. يمكن استعماله إما لوحده أو إلي جانب AH. يشتغل ESP باستعمال البروتوكول TCP علي المنافذ 50 و 51 وهو موثّق في المستند RFC 2406 .

Ethernet: تخطيط شبكة اتصال محلية (LAN) يعتمد على طريقة يطلق عليها Carrier Sense Multiple Access/Collision Detection (الوصول المتعدد لتحسس الحامل / اكتشاف العارض).

تأتى Ethernet فى عدة أشكال- تتوفر المواصفات فى IEEE.802.3 ومع ذلك توجد إصدارات أخري منها. تعد Ethernet هى تخطيط الشبكة الأكثر شيوعا فى العالم فى الوقت الحالي.

Extranet VPNs (شبكات VPN الاكسترانت) : نوع من الشبكات VPN يتيح إنشاء اتصالات آمنة مع الشركاء المهنيين والموردين والعملاء بهدف إجراء تجارة الكترونية. شبكات VPN الاكسترانت هي ملحق لشبكات VPN الانترانت مع إضافة جدران النار لحماية الشبكة الداخلية.

Fail over (التقدم من الفشل) : الامتداد المنطقى لتحمل الخطأ. فى هذا النظام ، يوجد خادمان (أو أكثر)، على كل منهما نسخ مطابقة من محركات أقراص وموارد الخادم الرئيسى . إذا فشل الخادم الرئيسي. يتولى الخادم الاحتياطي الأمر ديناميكيا ، ولا يرى المستخدمون الفرق على الإطلاق (باستثناء حدوث بطء بسيط وقصير).

Fast Ethernet: إصدار محدث من Ethernet يزيد من سرعة النقل من 10 إلى 100mbps ، مع المحافظة على كل العناصر المميزة لـ Ethernet تقريبا.

FAT32 : بنية أفضل من نظام الملفات القديم والمعروف باسم FAT لتتبع مواضع الملفات على القرص الصلب تستخدم فى Windows 98 أو الإصدارات الأحدث .

FDDI : اختصار لعبارة Fiber Distributed Data Interface (واجهة بيانات ألياف موزعة)، وهى طريقة لإرسال البيانات عبر شبكة باستخدام الليزر ونبضات الضوء التى يتم إرسالها عبر كبل ألياف زجاجية بدلا من إرسال الكهرباء عبر سلك نحاسى .

fiber (**ألياف**): يتم استخدام الألياف البصرية بدلا من الأسلاك النحاسية فى بعض الشبكات . يبدو ذلك مثل كبل محورى به خيوط مرنة من الزجاج فى المنتصف بدلا من الأسلاك النحاسية .

Fiber optic (**ليف بصرى**): تقنية لكبلات الشبكات تستخدم إشارات تتألف من نبضات ضوئية بدلا من الشحنات الكهربية المستخدمة فى الكبلات النحاسية.

Fire Wall (**جدار النار**) : هو عبارة عن كمبيوتر أو برنامجاً متخصصاً أو أى جهاز آخر يتحكم فى الوصول إلي الانترنت المتصل بالشبكة حيث تتصل موارد الشبكة الخصوصي بالانترنت العمومية ويحمي الكمبيوترات الشبكية من الأعمال العدائية التي يمكن أن تهدد الكمبيوترات الداخلية، مما سيؤدي إلي تشوه البيانات أو حرمان المستخدمين المرخصين من الخدمة. يشبه جدار نار من القرميد مصمم عند إحدي جهتي المبني يمنع النار من الانتشار إلي جزء آخر من المبني. أي نيران يمكن أن تثور داخل المبني ستتوقف عند جدار النار ولن تنتشر إلي الأجزاء الأخري للمبني لذا تنعقد الآمال علي أن يوقف جدار نار الشبكة أي هجوم عليها.

FQDN (Fully qualified domain name) (**اسم نطاق مؤهل بصورة تامة**) : هو اسم يتم تعيينه لنطاق أو مضيف على الانترنت . تُعرِّف Domain Name Service (خدمة أسماء النطاق) التسلسل الهرمى لكيفية تحديد FQDN.

Frame (**إطار**): وحدة البيانات التى تبنيها ، ترسلها وتستلمها بروتوكولات طبقة ربط البيانات مثل Ethernet و Token Ring. تنشىء بروتوكولات طبقة ربط البيانات الأطر عن طريق تغليف البيانات التى تستلمها من بروتوكولات طبقة الشبكة ضمن ترويسة وتذييل.

Frame relay (**نقل الأطر**) : طريقة لإعادة تأطير (أو إعادة تحزيم) البيانات التى تم تحزيمها بالفعل لتمكينها من أن يتم إرسالها عبر شبكة نقل الأطر الخاصة بشركة الهاتف .

FTP : اختصار لعبارة File Transfer Protocol (بروتوكول نقل الملفات)، وهو جزء من مجموعة بروتوكولات TCP/IP الذى يمكن المستخدمين من نسخ الملفات بين أجهزة الكمبيوتر .

Full backup (**النسخ الكامل**): عملية نسخ الملفات الموجودة على القرص الصلب ، سواء تم تعديل الملفات منذ آخر نسخة احتياطية تم إنشاؤها أم لا . (انظر differential backup) .

Full-duplexing (**مزدوج كامل**): شكل لاتصالات الشبكات يستطيع فيه النظامان المتصلان ببعضهما إرسال إشارتهما فى نفس الوقت.

Gateway (**مدخل**) : مصطلح عام لوصف نظام يصل- بصفة أساسية- نظامين . يمكن أن تمرر المداخل البريد وتترجم البرتوكولات وتعيد إرسال حزم البيانات وتجرى مهام أخرى.

Gateway protocols (**بروتوكولات مدخل**): هى أعضاء فى مجموعة برتوكولات TCP/IP التى تستخدمها الموجهات لتحديد أفضل مسار توجيه لحزم البيانات .

Gbps: **جيجا بت فى الثانية**. : وحدة تستخدم عادة لقياس سرعة النقل على الشبكة، كما تستخدم لقياس سرعة أجهزة تخزين البيانات.

Gigabit Ethernet: آخر إصدار من بروتوكول طبقة ربط البيانات Ethernet ، يعمل بسرعة 1,000 mbps

Group account (**حق دخول المجموعة**) : هو حق دخول يجمع بين حقوق دخول جميع المستخدمين المشتركة فى نفس حقوق الوصول .

GUI : اختصار لعبارة Graphical user interface (واجهة استخدام رسومية) ، وهى معالج أوامر على نظام تشغيل الكمبيوتر يمثل البيانات رسوميا . يعد Windows وواجهة Mac OS و Motif الخاصة بنظام UNIX واجهات استخدام رسومية .

Half-duplexing (**نصف مزدوج**): شكل لاتصالات الشبكات يستطيع فيه النظامان المتصلان إرسال الإشارات فى اتجاه واحد فقط كل مرة.

Header (**رأس**): جزء من حزمة بيانات تحمل معلومات عن مصدر حزمة البيانات ووجهتها ، ومجموع الاختبار ، وأية بيانات أخرى عن حزمة البيانات .

Hexadecimal notation (**رموز سداسية عشرية**): رموز الأساس 16. فى الرموز السداسية عشرية ، يمكنك العد من 0 إلي 15، كما يلى : F,E,D,C,B,A,9,8,7,6,5,4,3,2,1,0.

HTML : اختصار لعبارة Hypertext Markup Language (لغة ترميز النص التشعيبى) ، وهى طريقة لتنسيق النص العادى حتى يمكن عرضه بصفته نصا رسوميا فى نافذة برنامج استعراض . تستخدم HTML علامات أو أوامر تنسيق داخلية ، لتحديد الشكل الذى سوف تبدو عليه الأشياء.

HTTP : اختصار لعبارة Hypertext Transfer Protocol (برتوكول نقل النص التشعيبى) ، وهو جزء من مجموعة بروتوكولات TCP/IP يتم استخدامه لإرسال مستندات شبكة الويب العالمية عبر الانترنت.

Hub (**وحدة توصيل مركزية**): جهاز توصل معه الكبلات الموصلة مع الكمبيوترات والأجهزة الأخرى، فتشكل كلها شبكة محلية. فى معظم الحالات، يشير المجمع المركزى إلى مكرر Ethernet معدد المنافذ وهو جهاز يضخم الإشارات التى يستلمها من كل جهاز متصل به ويوجهها إلى كل الأجهزة الأخرى فى نفس الوقت.

Hub (**وحدة توزيع**): جهاز يوفر اتصالاً مركزيا لشبكة سلكية . لا تُحسِّن وحدات التجميع من الإشارات أو توجهها ، ولكنها توفر فقط نقطة اتصال مركزية .

Hybrid network (**شبكة مختلطة**): شبكة تستخدم إستراتيجيات اتصال سلكية ولاسلكية .

IDE : اختصار لعبارة Integrated Drive Electronics (الكترونيات محرك الأقراص المتكاملة) ، وهى طريقة لإرفاق محركات أقراص صلبة بأجهزة كمبيوتر باستخدام منطق مضمن فى محرك القرص الصلب بدلا من استخدام جهاز آخر .

IEEE (Institute of Electrical and Electronic Engineers) (**معهد مهندسى الكهرباء والالكترونيات**): معهد تأسس عام 1984، متخصص بتطوير ونشر المعايير فى مجال الكمبيوتر والالكترونيات.

IMAP : اختصار لعبارة Interactive Mail Access Protocol (برتوكول الوصول إلي البريد التفاعلى)، وهو جزء من مجموعة بروتوكولات TCP/IP التى تتعامل مع إرسال البريد بين الخادم والوحدة التابعة . يحل IMAP محل POP بصورة كبيرة ؛ ويعد الإصدار الحالي منه هو IMAP4 .

Incremental backup (**نسخ إحتياطى تصاعدى**): مهمة نسخ احتياطي تستخدم مرشحا يجعلها تأخذ نسخا احتياطية فقط للملفات التى تم تعديلها منذ آخر مهمة نسخ احتياطي.

Indirect route (**مسار غير مباشر**): إرسالية للبروتوكول IP إلى الوجهة على شبكة أخرى ، يحدد فيها الحقل Destination Address فى ترويسة بروتوكول طبقة ربط البيانات كمبيوترين مختلفين.

Intermediate system (**نظام انتقالي**): على شبكات TCP/IP، موجه يوجه الإشارات المتولدة عن نظام طرفى من شبكة لأخرى.

Internetwork (**شبكة جامعة**): مجموعة من الشبكات المحلية (LANs) و/أو الشبكات الواسعة (WANs) المتصلة ببعضها بحيث يستطيع أى كمبيوتر أن يرسل إلى أى كمبيوتر آخر.

IP: اختصار لعبارة Internet Protocol (بروتوكول الانترنت)، وهو جزء من بروتوكول TCP/IP المسؤول عن توفير خدمات عنونة وتوجيه لحزم البيانات. يتأكد IP من أن حزم البيانات تتم عنونتها بصورة مناسبة .

IP address (**عنوان IP**): سلسلة من الأرقام المرتبطة بعنوان MAC لمحول الشبكة . يبلغ طول هذا العنوان 32 بت ويتم تقسيمه إلي أربع سلاسل يبلغ كل منهما 1 بايت التي تتراوح قيمتها من 0 إلي 255 .

IP Security Protocol (IPSec) (**بروتوكول أمان IP**): مجموعة من بروتوكولات TCP/IP مصممة لتعطى اتصالات مشفرة على طبقة الشبكة . لكى تتواصل الكمبيوترات باستخدام IPSec ، يجب أن تتشارك على مفتاح عام.

IPX : اختصار لعبارة Internetworking Packet Exchange (تبادل حزمة بيانات الشبكات الداخلية) ، وهو جزء من برتوكول IPX/SPX الخاص بـــــــ Novell NetWare والمسؤول عن العنونة والتوجيه .

IRQ : اختصار لعبارة Interrupt Request (طلب مقاطعة) ، وهو طلب للمعالج بأن يمنح انتباها للجهاز الطالب . يتم تعيين IRQ مختلف لكل جهاز من أجهزة الكمبيوتر .

ISAMKP اختصار لعبارة Internet Security Association and Key Management Protocol (**اقتران أمان الانترنت وبروتوكول إدارة المفتاح**) : هيكل يعرف آليات تطبيق بروتوكول تبادل مفتاح والتفاوض علي أسلوب أمان. يستعمل ISAMKP للتبادلات الآمنة لبارامترات اقتران الأمان وللمفاتيح الخصوصية بين النظراء في بيئة IPSec، وكذلك إنشاء المفتاح وإدارته.

ISDN : اختصار لعبارة Integrated Services Digital Network (الشبكة الرقمية للخدمات المتكاملة) ، وهى خدمة هاتف رقمى مبدل . لقد توقف استخدام ISDN وتم استبدالها بتكنولوجيا حديثة ، مثل : DSL واتصالات نطاق واسع باستخدام الكبل مودم .

ISP : اختصارات لعبارة Internet service Provider (مزود خدمة الانترنت) ، وهى شركة توفر اتصالات للانترنت .

Jumper (**وصلة تخطى**): جزء بلاستيكى صغير جدا (أقل من 1/8 بوصة على الجانب) بداخله شريط معدنى موصل. يتم استخدام وصلات التخطي . (مثل رموز التبديل) لتأسيس اتصالات كهربية على بطاقة .

Kbps: كيلو بايت فى الثانية . وحدة قياس تستخدم عادة لقياس سرعة النقل على الشبكة.

LAN: اختصار لعبارة Local area network (شبكة اتصال محلية) ، وهى مجموعة من أجهزة الكمبيوتر فى منطقة محلية ترتبط معا دون أية موجهات بينها . تتصل كل أجهزة الكمبيوتر بنفس مجموعة وحدات التجميع (Hubs) أو مبدلات (Switches) فى LAN، وتعد كل موارد الشبكة محلية ، وتعمل بالسرعة الكاملة للشبكة .

Late collision (**تصادم متأخر**): على شبكة Ethernet، تصادم بين رزمتين يحدث بعد أن تغادر إحدى الرزمتين أو كلاهما النظام المرسل.

Link state protocol (**بروتوكول حالة الربط**): بروتوكول توجيه ديناميكى يقيس الفعالية النسبية لمسارات الشبكة عن طريق خصائص الارتباطات التى تتيح الوصول إلى الجهة.

Linux: نظام تشغيل مجانى يشبه UNIX تم تطويره على يد Linus Torvalds ومجموعة من مبرمجى الانترنت. يعد Linux نظام تشغيل مجانيا وسريعا ومستقرا .

Log in (**تسجيل الدخول**) : **انظر Log on**

Log on : مصطلح يشير إلى قيام المستخدم بتعريف نفسه على الشبكة (أو على وحدة خدمة معينة فى الشبكة) وحصوله على إمكانية الوصول إلى مواردها .

Log out (**إنهاء الاتصال**): عملية الخروج من الشبكة . وبهذا تصبح جميع الأقراص الصلبة أو الطابعات التى كنت متصلا بها غير متاحة لك .

Logon name (**اسم تسجيل الدخول**) : يشير فى الشبكات Windows إلى الاسم الذى يعرف المستخدم بصورة فريدة على الشبكة ، يعرف أيضا باسم المستخدم أو معرف المستخدم .

Mac OS X : أحدث وأفضل نظام تشغيل لأجهزة Macintosh .

Mac OS X Serve : أفضل نظام تشغيل تابع لشركة Apple لوحدات خدمة Macintosh

Mail server : (وحدة خدمة البريد الالكتروني) : يشير إلى وحدة الخدمة التى تخزن فيها رسائل البريد الالكتروني . يمكن أن يستخدم نفس الجهاز كوحدة خدمة ملفات أو طباعة أو أن يتم تخصيصه كوحدة خدمة بريد الكتروني .

MAN (Metropolitan area network) (**شبكة عاصمة**): شبكة بيانات تخدم منطقة أكبر من المنطقة التي تغطيها الشبكات المحلية (LAN) وأصغر من المنطقة التي تغطيها شبكة واسعة (WAN). معظم شركات MAN المستخدمة اليوم تخدم مجتمعات أو بلدان ، أو مدن .

Mbps: ميجا بت في الثانية. وحدة تستخدم عادة لقياس سرعة النقل على الشبكة.

Media (**وسيط**): في مجال الشبكات ، مصطلح يستخدم لوصف ألية مادية لعمل البيانات تستخدمها الكمبيوترات والأجهزة الأخرى على الشبكة إرسال البيانات لبعضها . في الكمبيوترات ، مصطلح يستخدم للإشارة إلى أدوات التخزين الدائم للبيانات ، مثل الأقراص الصلبة والمرنة.

Metric (**مترى**): حقل في جدول توجيه على كمبيوتر TCP/IP يحتوى على قيمة تقيس الفعالية النسبية لمسار معين.

Multicast (**بت متعدد**): رسالة على الشبكة يمثل عنوان الوجهة فيها مجموعة من الكمبيوترات.

Multifunction cable tester (**أداة اختبار الكبلات متعددة الوظائف**): جهاز إلكتروني يختبر مجموعة من خصائص الكبل ، يقارن النتائج بمعايير معدة مسبقة عليه ويبين إن كان الكبل يعمل ضمن المعايير المحددة.

Multitasking (**تعدد المهام**): في نظام التشغيل ، هي القدرة على تقسيم وقت جهاز الكمبيوتر بين برنامجين عاملين أو أكثر في نفس الوقت .

NAT اختصار لعبارة Network Address Translation (**ترجمة عناوين الشبكة**) : يُمكِّن عددا من أجهزة الكمبيوتر تستخدم عناوين IP خاصة من التفاعل مع الانترنت عبر عنوان IP واحد عام . تختفي أجهزة الكمبيوتر بصفة أساسية خلف نظام تأميني أو خادم نائب يستخدم NAT ، ويتم توصيفه باستخدام عنوان IP العام .

NAT (Network Address Translation) (**ترجمة عناوين الشبكة**): تقنية جدار نارى تمكن عملاء TCP/IP من استخدام عناوين IP غير مسجلة للوصول إلى الانترنت.

NDS : اختصار لعبارة Network Directory Services (خدمات دليل Network) ، وهي مجموعة من المقاييس لتنظيم شبكات المشروعات . تعد هذه الخدمة ملكية خاصة لشركة Novell ، ولكنها متوفرة على العديد من النظم . تتسم هذه الخدمة بالقوة فيما يتعلق بتنظيم الشبكات وتجزئتها منطقيا .

NetBEUI : اختـــصار لعبـــارة NetBIOS Extended User Interface (واجهـــة اســـتخدام NetBIOS الممتدة) ، وهي امتداد لـــ NetBIOS يشمل القدرة على تأطير حزم البيانات ، بالإضافة إلي ميزات أخرى موسعة . يعد NetBEUI تنفيذ شائع لــــــــــــ NetBIOS .

NetBIOS : اختصار لعبارة Network Basic 1/0 System (نظام الإدخال/ الإخــراج الأساســي للشبكة) ، وهو برتوكول صغير غير قابل للتوجيه تم تطويره بواسطة IBM من اجل شبكات أجهزة الكمبيوتر الشخصية الصغيرة .

NetWare : نظام تشغيل شبكات Novell . يتسم هذا النظام بالقوة وقابلية التحجيم بدرجة عالية ، كما أنه معقد لدرجة تجعل من الصعب إدارته ، ولكنه شديد السرعة .

Network (**شبكة**): مجموعة من أجهزة الكمبيوتر المتصلة بواسطة تخطيط عام يمكِّن إرسال البيانات .

Network access point (**نقطة وصول للشبكة**): نقطة اتصال على شبكة الاتــصالات الرئيــسية للانترنت.

Network Adapter (**محول شبكة**): بطاقة محول يتم تركيبها فى جهاز الكمبيوتر ؛ حيث تــسمح لــه بالاتصال على الشبكة.

Network layer (**طبقة الشبكة**): الطبقة الثالثة فى نموذج OSI المرجعى . البروتوكولات التى تعمل على هذه الطبقة مسئولة عن تغليف بيانات طبقة النقل ضمن مخططات بيانية ، عنونتــها إلى وجهتــها النهائيــة ، توجيهها عبر الشبكة الجامعة وتجزئة المخططات البيانية عند الحاجة.

Network resource (**موارد الشبكة**) : يشير هذا المصطلح العام إلى محرك الأقراص أو الطابعات أو أى جهاز أخر موجود على أو متصل بوحدة الخدمة ويشترك فيه المستخدمون . فى المقابل ، تشير الموارد المحلية إلى أجهزة موجودة على أو متصلة بجهاز المستخدم نفسه .

NFS : اختصار لعبارة Network File System (نظام ملفــات الــشبكة)، وهـــو طريقـــة Sun Microsystems القياسية للسماح لجهاز كمبيوتر بالوصول إلي الملفات الموجودة على محرك قرص صـــلب لجهاز كمبيوتر آخر كما لو كانت الملفات جزءا من نظام الملفات المحلى .

NIC : اختصار لعبارة Network Interface Card (بطاقة واجهة الشبكة) ، وهى بطاقة إضافية يــتم توصيلها بجهاز كمبيوتر وتمكنه من الاتصال بالشبكة .

Node (**عقدة**): أي جهاز يمكن عنونته بشكل فريد على شبكة . كــــكــــمبيوتر أو موجه أو طابعة.

NOS : اختصار لعبارة Network Operating System (نظام تشغيل شبكات) ، وهو برنامج يمكن جهاز الكمبيوتر من أداء مهام معينة مركزية للشبكة ، تعـد Netware و Unix و Windows Server نظم تشغيل شبكات .

Novell : الشركة المصممة لنظام تشغيل NetWare

Octet (**ثمانى**) : الاسم الرسمى للبايت (ثمانى بتات ، أو ثمانية أرقام ثنائية في صور 1 , 0) .

Open Standards (**مقاييس مفتوحة**): مقاييس الأجهزة والبرامج التى لا تعد ملكية خاصة لأية شركة مصنعة. يعد TCP/IP و Ethernet مقاييس مفتوحة .

Operating System (**نظام تشغيل**): البرنامج الذى يمكّن جهاز الكمبيوتر المستخدم مـن الاتـصال بالأجهزة وتنفيذ المهام. يعد كل من UNIX و Windows نظم تشغيل .

Optical Fiber (**ألياف بصرية**) : الوسط الذى تستخدمه شبكات الألياف البصرية . تستخدم معظـم الشبكات إما كبل محورى أو UTP.

OSI model (**نمـوذج OSI**) : اختـصار لعبـارة Open System Interconnect Model (النموذج المرجعي لاتصالات الأنظمة المفتوحة) ، وهو نموذج مرجعي يفصِّل الطبقـات الـسبع لوظـائف الشبكات . يقدم نموذج OSI طريقة مثالية لفهم نظرية ربط الشبكات .

OSPF : اختصار لعبارة Open Shortest Path First (فتح أقصر مسار أولا) ، وهو بروتوكـول توجيه يستخدم ما يطلق عليه لوغاريتم حالة الارتباط على مسارات التوجيه المتوفرة التى يمكـن أن تـسلكها حزمة البيانات إلي وجهتها ، وتحدد أفضل مسار توجيه . لا يتوفر لـــــ OSPF أقصى عدد للقفزات مثل RIP .

Pack Filtering (**تصفية الرزم**) : أحد أقدم أنواع تقنيات فحص الرزم وأكثرها شيوعاً، تبـدأ تـصفية الرزم بفحص محتويات الرزمة لتحديد ما إذا كانت المحتويات تطابق المعايير بناءً علي مجموعة محددة مسبقاً من القواعد. إذا كانت محتويات الرزمة تطابق تلك القواعد، يسمح للرزمة بالمرور ويتم التخلص من الرزمـة إذا كانت المحتويات لا تطابق قواعد تصفية الرزم المحددة مسبقاً.

Packet (**حزمة بيانات**): يطلق عليها أيضا مخطط بيانات ؛ وهى المعلومات التى يتم وضعها فى مغلف يطلق عليه رأس. تحتوى حزم البيانات على رؤوس (التى تعالج العنونة) وتصحيح خطأ ومجاميع اختبار ويـتم فى النهاية إرسال البيانات عبر الشبكة .

Packet filtering (**تصفية الرزم**): تقنية جدار نارى يتم فيها تكوين الموجه بحيث يمنع أنواعا معينة من الرزم من دخول الشبكة.

Packet header (**رأس حزمة بيانات**) : انظر : header (رأس) .

Packet switching (**مبادلة حزم البيانات**): أحد أنواع اتصالات الشبكة يتم فيه تجزئة الرسائل إلى وحدات صغيرة وإرسالها إلى وجهتها.

Parallel Port (**منفذ متوازي**): منفذ يستخدم عادة لربط الطابعات بأجهزة الكمبيوتر، لذا يطلق عليه أحيانا اسم منفذ الطابعة. تعمل منافذ parallel على إرسال البيانات عبر ثمانية أسلاك على **دفعات** ، بحيث يتم نقل بايت واحد فى كل دفعة . انظر (serial port) .

Partition (**جزء**): يتم تقسيم القرص الصلب الواحد إلى أجزاء متعددة صغيرة، يتعامل معها نظام التشغيل على أنها محركات أقراص مستقلة .

password (**كلمة المرور**): كلمة سرية تخصص لكل شخص علي حده لضمان حماية جهازك وملفاتك من أية محاولة تسلل إليها . كلما أحيطت هذه الكلمة بقدر أكبر من السرية ، كلما توفرت حماية أكبر لملفاتك.

Peer- To- Peer (**نظير بنظير**): شبكة يتم إنشاؤها بدون خادم مركزى (وحدة مركزية) . فى الشبكة النظيرة ، يمكن أن تكون كل أجهزة الكمبيوتر خادمات ووحدات تابعة على حسب الضرورة . تعد هذه الشبكات مفيدة بالنسبة للشبكات الصغيرة .

Permissions (**الصلاحيات**): الحقوق التى تمنح لمستخدم معين أو مجموعة من المستخدمين للسماح لهم بالوصول إلى ملفات بعينها .

Physical layer (**الطبقة الفيزيائية**): أسفل طبقة فى نموذج OSI المرجعى وهى تعرف طبيعة وسيط الشبكة ، كيف يجب تنصيبه وما أنواع الإشارات التى يجب حملها.

POP : اختصار لعبارة Post Office Protocol (بروتوكول مكتب البريد) ، وهو مقياس TCP/IP لإرسال البريد بين وحدة الخدمة والوحدة التابعة . يعد POP3 هو الإصدار الحالي من POP .

Post Office Protocol 3 (POP3) (**بروتوكول مكتب البريد 3**): بروتوكول من TCP/IP يعمل على طبقة التطبيق ويستخدمه عملاء البريد الالكتروني لتحميل الرسائل من ملقمات البريد الالكتروني.

POTS : اختصار لعبارة Plain Old Telephone Service (خدمة الهاتف القديمة العادية)، وهـي نغمة الاتصال القديمة العادية المستخدمة للأصوات وأجهزة المودم .

PPP : اختصار لعبارة Point- To- Point Protocol (بروتوكول نقطة إلي نقطة) ، وهو جزء من مجموعة بروتوكولات TCP/IP يتم استخدامه لتوصيل أجهزة الكمبيوتر عبر خطوط هاتف مبدلـة – إمـا خدمة هاتف عادية (POTS) أو خدمة رقمية مبدلة (ISDN) .

pptp اختصار لعبارة Point- To- point tunneling protocol (بروتوكول استخدام الأنفاق من نقطة– لنقطة): بروتوكول يعمل على طبقة ربط البيانات ويستخدم لتقديم اتصالات آمنـة للـشبكات الخاصة الافتراضية (VPN).

Presentation layer (**طبقة التقديم**): الطبقة الثانية من الأعلى فى نموذج OSI المرجعى وهى مسؤولة عن ترجمة الصيغ التى تستخدمها مختلف أنواع الكمبيوترات على الشبكة.

Protocol (**برتوكول**): مقياس متفق عليه . بمصطلحات ربط الشبكات ، يتم استخدام البرتوكول لعنونة استلام البيانات عبر الشبكة والتأكد منه .

Protocol Translator (**مترجم برتوكول**): جهاز يمكنه الترجمة بين برتوكولي شبكة . عـادة مـا تترجم أدوات ترجمة البرتوكولات NetWare IPX إلي TCP/IP، حتى يتمكن المستخدمون على شـبكة IPX من الوصول إلي موارد الانترنت أو IP .

Proxy Server (**خادم نائب**): خادم يخفى عناوين IP للشبكة الداخلية من الانترنت، عن طريق تقـديم طلبات للوحدات التابعة الداخلية.

RAID : اختصار لعبارة Redundant Array of inexpensive Disks (مصفوفة متكـررة مـن الأقراص غير المكلفة) وهو يشير إلي مجموعة من محركات الأقراص الصلبة المرتبطة معاً، والتي يتم التعامل معها كأنها محرك أقراص واحد. يتم توزيع البيانات علي محركات أقراص متعددة، يحتوي أحدها علـي معلومـات تدقيق للاستفادة منها في إعادة إنشاء البيانات في حالة حدوث أي خطأ بأحد محركات الأقراص .

Redirection (**إعادة التوجيه**) : أحد المصطلحات الرئيسة المستخدمة فى الشبكات . تبعا لعملية إعادة التوجيه ، يبدو أى جهاز واقع على الشبكة ، كالقرص الصلب أو الطابعة ، كأنه جهاز محلى . يعترض برنامج الشبكة المستخدم على جهازك طلبات I/O الموجهة إلى هذا الجهاز ويعيد توجيهها إلى الشبكة .

Registry (**السجل**): الملف الذى يحتفظ فيه نظام Windows بمعلومات التهيئة .

Remote Access VPN (**الشبكة VPN للوصول البعيد**) : نـوع مـن الـشبكات VPN يتـيح للمستخدمين الهاتفيين الفرديين الاتصال بموقع مركزي علي الانترنت أو خدمة شبكة عمومية أخري بطريقـة آمنة . هذا النوع من الشبكات VPN هو اتصال مستخدم – بشبكة LAN يتيح للموظفين الذين يحتـاجون إلي الاتصال بشبكة الشركة من الخارج .

Remote node (**وحدة فرعية جديدة**): جهاز كمبيوتر يتصل بالشبكة عبر استراتيجية وصول عن بعد، مثل : الاتصال الهاتفى أو Virtual Private Networking (ربط الشبكات الظاهرية الخاصة) .

Repeater (**جهاز تكرار الإشارات أو مكرِّر**) : جهاز يمكن الشبكات من الاتصال بـصورة جيـدة . يضخم المكرِّر الإشارات الرقمية ، ويعيد إرسالها نحو وجهتها بهدف زيادة المسافات التي يمتد عبرها الكابل بين وحدتين

RG58: أحد أنواع الكبلات المحورية ، يعرف أيضا باسم Thin Ethernet وهو محدد فى مواصفة DIX Ethernet الأصلية.

RG8: أحد أنواع الكبلات المحورية ، يعرف أيضا باسم Thick Ethernet وهو محدد فى مواصفة DIX Ethernet الأصلية.

RIP : اختصار لعبارة Routing Information Protocol (برتوكول معلومـات التوجيـه)، وهـو برتوكول يعمل عن طريق حساب عدد مرات تحرك حزمة بيانات نحو وجهتها . يطلق على كل توجيه جديد اسم فقرة ، وعادة ما يتم تعيين أقصى عدد للقفزات إلي 16. فى RIP ، اذا تم توجيه حزمة بيانات أكثر من 16 مرة ، يتم تجاهلها .

RJ11: وصلة بأربع أو ست دبابيس تستخدم فى شبكات الهاتف.

RJ45: وصلة بثمانية دبابيس تستخدم فى شبكات الهاتف . غالبية الشبكات المحلية اليوم تستخدم وصـلات RJ45 مع كبل UTP.

Router (**موجه**) : جهاز أو برنامج (اختياري) يوجه حزم البيانات نحو وجهتها. يجب توصيل الموجهـات بشبكتين على الأقل . تحدد الموجهات كيفية إرسال البيانات اعتمادا على ظروف العمل .

Routing tables (**جداول التوجيه**) : قاعدة بيانات لمسارات التوجيه بين الـشبكات الـتي تحملـها الموجهات فى الذاكرة الخاصة بها . بصفة عامة ، كلما صغر حجم جداول التوجيه ، زادت سرعة الموجة .

SCSI : اختصار لعبارة Small Computer System interface (واجهة نظام كمبيوتر صـغير) ،

وهي طريقة لتوصيل مجموعة مختلفة من الوحدات الطرفية بجهاز كمبيوتر . تشتمل أجهزة SCSI على محركات الأقراص الصلبة ومحركات الأقراص المدمجة والماسحات الضوئية ، وغيرها .

Segment (**المقطع**) : يشير إلى جزء واحد فقط من الكابل يمكن أن يربط أكثر من جهازى كمبيوتر ، مع استخدام عنصرى مقاوم عند طرفى الكابل .

Serial port (**منفذ متسلسل**) : هو منفذ يستخدم عادة لربط مودم أو ماوس بجهاز كمبيوتر. يطلق عليه أحيانا اسم منفذ الاتصالات . (انظر parallel port) .

Server **وحدة خدمة (خادم)** : جهاز كمبيوتر على شبكة يشترك فى مورد محدد (ملف أو طباعة أو تطبيقات) مع أجهزة كمبيوتر أخرى .

Session layer (**طبقة الجلسة**) : إحدي طبقات نموذج OSI السبعة، وتختص بجلسات الاتصال بين وحدات الشبكة .

Share name (**اسم عملية المشاركة**): اسم يتم تخصيصه لمورد الشبكة عند مشاركته . يعتمد مستخدمو الشبكة الآخرين على هذا الاسم للوصول إلى المورد المشترك .

Shared folder (**الجلد المشترك**): يشير إلى محرك أقراص وحدة الخدمة أو مجلد فى هذا المحرك يتم مشاركته بين جميع الأجهزة على الشبكة حتى تتمكن من الوصول إليه .

Shared resource (**المورد المشترك**): يشير إلى مورد ، كالقرص أو الطابعة ، يتم إتاحة الوصول إليه لجميع مستخدمي الشبكة.

Shell (**معالج أوامر**) : واجهة استخدام تفاعلية فى نظام تشغيل أو نظام تشغيل شبكات. يأخذ معالج الأوامر أمر المستخدم عند سطر الأمر (على سبيل المثال: محث C فى DOS) أو من خلال واجهة استخدام رسومية

(على سبيل المثال : واجهة Windows) ، ويمررها إلي نظام التشغيل أو نظام تشغيل شبكات .

Shielded twisted pair (**الكابل المزدوج الملتف المعزول**): كابل مكون من سلكين ملتفين محاط بغطاء . يستخدم عادة فى شبكات Token Ring ويعرف أيضا باسم STP . انظر Twisted pair .

Short circuit (**دائرة قصر**): مشكلة فى الكبلات تحدث نتيجة تماس ناقلين أو أكثر داخل الكبل.

Site – to Site (**الشبكات VPN بين المواقع**) : نوع من الشبكات VPN يستعمل لتمديد شبكة LAN موجودة لشركة إلي أبنية ومواقع أخري من خلال استعمال معدات مكرسة لكي يتمكن الموظفون البعيدون في تلك الأماكن من أن يستخدموا نفس خدمات الشبكة. تعتبر هذه الأنواع من الشبكات VPN متصلة

بنشاط طوال الوقت. تسمي الشبكات VPN بين المواقع أحياناً بالشبكات VPN الجهازية، أو الانترانت، أو الشبكات VPN بين الشبكات LAN .

SLIP اختصار للعبارة Serial Line Internet Protocol (بروتوكول الانترنت ذو الخط التسلسلى): برتوكول من TCP/IP يعمل على طبقة ربط البيانات ويستخدم فى اتصالات WAN وخاصة باستخدام الطلب الهاتفى للاتصال بمزود خدمات الانترنت أو مزود آخر.

Slot interface (واجهة فتحة) : انظر card- slot interface (واجهة فتحة بطاقة) .

SMTP : اختصار لعبارة Simple Mail Transmission Protocol (برتوكول إرسال البريد البسيط) ، وهو مقياس TCP/IP لبريد الانترنت يتبادل SMTP البريد بين الخادمات، علي عكس POP الذي يرسل البريد بين وحدة الخدمة ووحدة تابعة.

SNMP اختصار للعبارة Simple Network Management Protocol (بروتوكول إدارة الشبكات البسيطة) : بروتوكول من TCP/IP يعمل على طبقة التطبيق ولغة استعلام يستخدم لإرسال معلومات عن حالة مكونات الشبكة إلى مركز لإدارة الشبكة.

Source IP Address (عنوان IP للنظام المصدر): حقل بطول 32 بت فى ترويسة IP يحتوى على قيمة تستخدم لتمييز محول الشبكة الذى صدرت الرزمة منه.

Split Tunneling (شق الأنفاق المنقسم) : طريقة يسمح بها لمستخدم أو لموقع VPN بعيد بالوصول إلي شبكة عمومية (الانترنت) في الوقت نفسه الذي يصل فيه إلي الشبكة VPN الخصوصية من دون بيانات الشبكة العمومية داخل النفق أولاً.

Star topology (تخطيط نجمى) : تخطيط شبكة يتم فيه تمرير كل الاتصالات من خلال جهاز مركزى يطلق عليه وحدة تجميع . يستخدم كل من FDDI و ATM و 10BASE-T و Token Ring تخطيطات نجمية .

Shielded twisted pair (STP) (زوج مجدول معزول): أحد أنواع الكبلات المستخدمة على الشبكات المحلية فى البيئات التى تحتاج لمزيد من الحماية من التشويش الكهرومغناطيسى.

Straight- through connection (وصلة مباشرة): نظام لتوصيل كبلات STP, UTP يتم فيه وصل كل واحد من الأسلاك الثمانية مع نفس التماس فى الوصلة على طرفى الكبل.

Striping (تخطيط): العملية التى تكتب فيها بطاقة وحدة تحكم فى محرك أقراص RAID بيانات إلي أقراص متعددة.

Subnet (**شبكة فرعية**) : طريقة لتقسيم شبكات TCP/IP إلي أجزاء أصغر حجما من أجل أغـــراض الإدارة أو التامين . يتم توصيل الشبكات الفرعية بواسطة موجهات .

Subnet mask (**قناع شبكة فرعية**) : قناع عشرى نقطى يتم استخدامه لتحديد أى جزء من عنـــوان IP هو معلومات الشبكة وأي جزء هو معلومات الوحدة الفرعية . على سبيل المثال : قـــد يكـــون لجهـــاز كمبيوتر عنوان IP التالي : 192.168.1.5 قناع الـــشبكة الفرعيـــة 255.255.255.0. يعـــد جـــزء 192.168.1 من العنوان هو عنوان الشبكة ، ويعد جزء 5. هو عنوان الجهاز المحدد على هذه الشبكة .

Switch (**مبدل**): جهاز لوصل الشبكة على مستوى طبقة ربط البيانات يشبه وحدة التجميـــع (Hub). يعمل هذا الجهاز على إرسال البيانات إلى المنفذ المتصل بالجهاز المستقبل لحزمة البيانات فقط بدلا من إرسالها إلى جميع المنافذ كما يفعل جهاز hub العادى .

TCP : اختصار لعبارة Transmission Control Protocol (بروتوكول التحكم فى الإرسال)، وهو جزء من مجموعة بروتوكولات TCP/IP التى تتأكد من تسليم حزم البيانات إلي وجهتـــها بـــصورة يمكـــن الاعتماد عليها .

TCP/IP اختصار لعبارة Transmission Protocol/Internet Protocol (بروتوكول التحكم فى الإرسال / بروتوكول الانترنت) ، وهو مصطلح عام لوصف مجموعة البرتوكولات متعددة الأوجه الـــتى تعمل باستخدامها الانترنت . يعد TCP/IP مقياسا مفتوحا أيضا ؛ ولا يمتلك هذا البروتوكول أية شـــركة . يمكن لأى شخص إنشاء تنفيذ لبرتوكول TCP/IP إذا كان يرغب فى ذلك .

Termination (**وصلة إنهاء**): وصلة ذات مقاومة تثبت على طرفى شبكة خطية لمنع الإشارات الواصلة إلى طرف الكبل . من الارتداد فى الاتجاه الأخر.

Thick Ethernet: تسمى أيضا 10Base 5 ، مواصفة Ethernet للطبقة الفيزيائية تستخدم كـــبلا محوريا من نوع RG8 فى بنية خطية ، تعمل بسرعة 10Mbps وبطول أقصى للكبلات هو 500 متر.

Thin Ethernet: تسمى أيضا 10Base ، مواصفة Ethernet للطبقة الفيزيائية تستخدم كبلا محوريا من نوع RG58 فى بنية خطية ، تعمل بسرعة 10Mbps وبطول أقصى للكبلات هو 185 متر.

Thinnet : اسم دارج آخر لشبكة 10BASE-2 Ethernet .

TI : خط هاتف رقمى يمكن أن يحمل البيانات بسرعات تصل إلي 544. 1 ميجابت فى الثانية.

Token Passing (**تمرير العلامة**): آلية MAC تستخدم فى الشبكات ذات البنية الحلقية وهى تـــستخدم

نوعا منفصلا من الأطر يسمى علامة (token) تدور عبر الشبكة من كمبيوتر لآخر.

Token Ring : تخطيط يتبادل البيانات بين أجهزة الكمبيوتر بواسطة تمرير رموز مميزة بدلا من CSMA/CD .

Topology (**بنية طبوغرافية**) : الطريقة المستخدمة لتوصيل كبلات الشبكة وربط الكمبيوترات بالكبلات.

Transceiver (**المرسل المستقبل**): جزء من بطاقة محول الشبكة يدير عملية إرسال حزم البيانات وتسلمها من أسلاك الشبكة.

Transport Layer (**طبقة النقل**) : الطبقة الرابعة في نموذج OSI المرجعي، تحتوي بروتوكولات تقدم خدمات تتم الخدمات التي تقدمها بروتوكولات طبقة الشبكة.

Tree (**تفرع**): على شبكة Microsoft التى تستخدم Active Directory (الدليل النشط) ، يتكون التفرع من نطاق جذرى ، وهو النطاق الأول الذى تضعه فى وضع الاتصال . يمكن أن تحتوى التفرعات على نطاق متعددة (بما فى ذلك النطاق الجذرى) . تعد النطاقات المضافة إلي التفرع نطاقات فرعية .

Tunneling (**استخدام الأنفاق**) : تقنية لإرسال البيانات عبر شبكة عن طريق تغليفها ضمن بروتوكول آخر.

Tunneling Protocol (**بروتوكول تغليف حزم البيانات**) : بروتوكول يتأكد من أن البيانات التى تمر عبر Virtual Private Network (شبكة ظاهرية خاصة) لشركة سوف تكون مؤمنة . يشبه تغليف حزم البيانات وضع رسالة / مظروف معنون إلي صندوق بريد شبكة غير محلية فى مظروف آخر أكبر يستخدم خدمة البريد لإرساله إلي موقع شركة أخرى . عندما يصل البريد إلي صندوق بريد الشركة غير المحلية ، يخرج البريد ثم يأخذ موظف البريد الرسالة من المظروف الكبير ويرسلها إلي الشخص المعنونة إليه .

Twisted pair (**كابل مزدوج ملتف**) : يتكون هذا الكابل من زوج أو أكثر من الأسلاك الملتفة معا بطريقة معينة تعمل على تحسين خصائص الكابل الكهربية . (انظر Shielded twisted pair و Unshielded twisted pair) .

UDP: اختار لعبارة User Datagram Protocol (بروتوكول مخطط بيانات المستخدم)، وهو جزء من مجموعة بروتوكولات TCP/IP الذى يتعامل مع تسليم لحزم البيانات لا يمكن الاعتماد عليه . أى أن UDP يتعامل مع تسليم حزم البيانات عبر ارتباطات لا تكون متوفرة دائما .

UNIX : نظام تشغيل تم تطويره فى أوائل السبعينات .

UPS : اختصار Uninterrupted power supply (مصدر الطاقة غير المنقطع). وهو جهاز يتـــصل ببطارية لتزويد جهاز الكمبيوتر بالطاقة بصورة تلقائية بمجرد انقطاع الطاقة الكهربية .

USB (Universal Serial Bus) (ناقل تسلسلي عالمي) : ناقل طرفي خارجي حل بـــسرعة محـــل الكثير من المنافذ الأخرى المستخدمة في الكمبيوتر.

User group (مجموعة مستخدمين): فى نطاقات Windows، فئة من مستخدمى النطاقات يتم تجميعهم معا من أجل توفير إدارة مبسطة . يتم إنـــشاء المجموعـــات وإدارتهـــا فى تطبيـــق User Manager for Domains (مدير المستخدمين للنطاقات) فى Windows.

UTP (Unshielded twisted pair) كبل مزدوج مجدول غير معزول : نوع من الكبلات يستخدم لشبكات الهاتف والبيانات ويتألف من ثمانية أسلاك نحاسية مجدولة في أربعة أزواج بمعدلات مختلفـــة ومغلفـــة بغمد عازل.

UTP : اختصار لعبارة Unshielded Twisted-Pair wire (سلك مزدوج مجدول غير محم) ، وهـــو كبل به أربعة أزواج من الأسلاك (أزرق وبرتقالي وأخضر وبنى) يتم استخدامه لتوصيل أسلاك شـــبكات Token Ring و Ethernet .

VPN اختصار للعبارة Virtual Private network (شبكة خاصة افتراضية) : تقنية للاتصال بشبكة من موقع بعيد باستخدام الانترنت كوسيط للشبكة.

WAN: اختصار لعبارة wide area network (شبكة اتصال واسعة)، وهى شبكة مكونـــة مـــن شـــبكتى LANs أو أكثر متصلين بواسطة خطوط هاتف (خطوط هاتف رقمية بصفة عامة)، ويتم توجيهها بين مقاطع.

Wi-Fi اختصار للعبارة Wireless Fidelity (الدقة اللاسلكية) : المصطلح الشائع الاستعمال لوصف الشبكات 802.11 اللاسلكية. يشير Wi-Fi أيضاً إلي شهادة صادرة عن Wi-Fi Alliance ، وهو اتحـــاد دولي لا يبغي الربح يتألف من باعة المنتجات 802.11. إن منتجات 802.11 التي تنال الشهادة Wi-Fi قد تم اختبارها ووجدت أنها قابلة للعمل بشكل متبادل مع المنتجات الأخرى المصادق عليها.

Wireless networking (التشبيك اللاسلكي) : مصطلح يشير إلي تقنية الراديو التي تمكن كمبيوترين أو أكثر من الاتصال باستعمال بروتوكولات الشبكة القياسية كـــ IP لكن دون كبلات.

Workgroup (مجموعة عمل) : المصطلح المستخدم بواسطة Microsoft للإشارة إلي شبكة نظير بنظير التى توفر مشاركة الملفات والطباعة . يتم تضمين إمكانات مجموعات العمل فى الإصدارات المختلفة من نظم تشغيل Windows .

كلمة أخيرة

أود قبل أن نفترق أن أشكرك علي متابعتك وصبرك علي قراءة هذا المرجع الشامل. وآمل أن تكون وجدت فيه الفائدة والمتعة التي تنشدها. ولقد بذلنا قصاري جهدي لإخراج هذا الكتاب في ثوب يحقق لك أكبر فائدة. ولذلك ولعموم الفائدة تجدني قد اسهبت في بعض الموضوعات واختصرت في أخري. اعتماداً علي أهمية الموضوع وأولوية استخدامه، وعلي حكمة القارئ العزيز وقدرته علي مسايرة الشرح .

فما كان من تقصير أو خطأ أو نسيان فهو مني ومن الشيطان، وما كان من توفيق وسداد فمن الله وحده " وما توفيقي إلا بالله" .

المرجع الأساسي لمستخدمي Windows Vista



يشرح هذا الكتاب واحداً من أحدث برامج التشغيل وهو Windows Vista ، ويتناول الكتاب الموضوعات التالية:

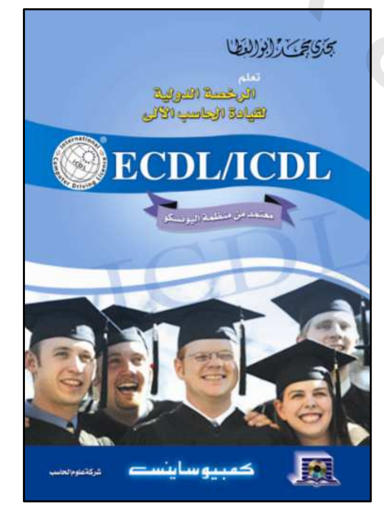
- *المزايا الجديدة فى Windows Vista.*
- *كيفية التعامل مع النوافذ والقوائم والحصول علي تعليمات المساعدة.*
- *استخدام قائمة "ابدأ" وشريط المهام والشريط الجانبي.*
- *التعامل مع البرامج والملفات والصور والأفلام وتعديلها وإضافة مؤثرات وخلفيات صوتية.*
- *التعامل مع ميزة التحكم الأبوي لحماية أطفالك من المواقع الهدامة والإباحية.*
- *كيفية الاتصال بالانترنت واستخدام مستعرض الانترنت لتصفح المواقع، واستخدام مركز المفضلة وتقييد المحتوي المثير للاعتراض وطباعة صفحات الويب أو إرسالها إلي الآخرين وكيفية استخدام بريد ويندوز (Windows Mail) .*
- *كيفية إعداد شبكة الاتصالات لتوصيل مجموعة أجهزة داخل منزلك أو شركتك.*
- *تحقيق الأمان عن طريق حماية جهازك من برامج التجسس والبرامج الخبيثة بواسطة Windows Defender أو العمل خلف جدار الحماية (Firewall)، والتحكم في حسابات المستخدمين User Account Control وتحديث البرنامج من خلال Windows Update .*
- *حماية بياناتك عن طريق النسخ الاحتياطي للبيانات واسترجاعها أو حتي النسخ الاحتياطي للجهاز كله وتعين نقاط استعادة النظام.*
- *تحقيق أقصي كفاءة للأقراص الصلبة وإدارتها عن طريق استخدام برامج الفراغات (Defragmentation) وتنظيفها (Clean Up) وضغط البيانات وتشفيرها.*
- *كيفية نسخ (Burn) الأفلام والصور وملفات الصوت إلي الأقراص المدمجة وكيف تنسخها (Rip) من الأقراص المدمجة إلي جهازك.*



تيسير Windows Vista

يعتبر كتاب تيسير Windows Vista دليل سهل ويغطي الموضوعات الآتية:

- *خلفية ضرورية تشمل التعامل مع الأطر والقوائم والمربعات الحوارية والحصول علي تعليمات المساعدة.*
- *استعراض وإدارة الملفات والمجلدات والبرامج.*
- *استخدام البرامج الملحقة والتعامل مع الصور والأفلام وملفات الصوت.*
- *التحكم في الطابعات والاتصال بالانترنت واستخدام المراقبة الأبوية لحماية الأطفال وبرامج الحماية فيه.*

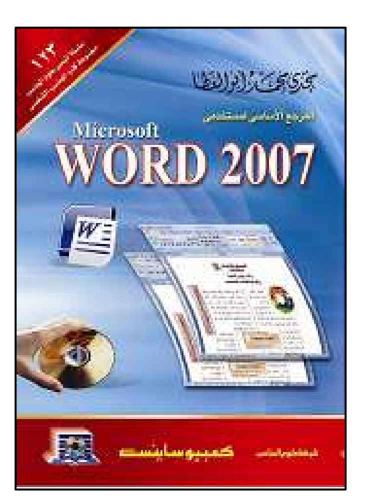


الرخصة الدولية لقيادة الحاسب الآلي ICDL

هذا هو الكتاب الذي يؤهلك للتقدم لأي من اختبارات شهادة الرخصة الدولية ECDL/ICDL. وهو الكتاب المعتمد من منظمة اليونسكو للتدريس في الدول العربية وهو يشتمل علي سبع وحدات كل وحدة في كتاب مستقل. هذه الوحدات هي :

- ✓ *المفاهيم الأساسية لتكنولوجيا المعلومات* ***Concepts of Information Technology (IT)***
- ✓ *استخدام الحاسب والتعامل مع الملفات* ***Using Computer and Managing Files***
- ✓ *معالجة النصوص* ***Word Processing***
- ✓ *جداول البيانات* ***Spreadsheets***
- ✓ *قواعد البيانات* ***Databases***
- ✓ *العروض التقديمية* ***Presentations***
- ✓ *الاتصالات وتكنولوجيا المعلومات* ***Information and Communications***

مرفق مع المجموعة قرص مدمج CD يحتوي علي الأمثلة والتمارين الواردة بالكتاب بالإضافة إلي نماذج للاختبارات السبعة للحصول علي شهادة ICDL .



المرجع الأساسي لمستخدمي Word 2007

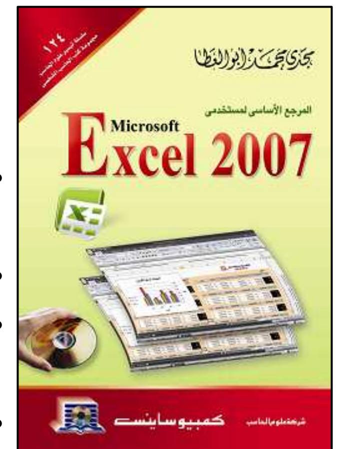
يشرح هذا الكتاب واحداً من أهم بــرامج مجموعــة Office 2007 وهو Word 2007، ويتناول الكتاب الموضوعات التالية:

- *المزايا الجديدة في Word 2007.*
- *مفاهيم تحرير المستندات وتنسيقها وتعديلــها ومراجعتــها وطباعتها.*
- *تصميم ونشر صفحات Web وإدراج الارتباطات التشعبية.*
- *تصميم مستندات تشتمل على الصور والرسوم والجــداول ومربعات النص. وكيفية إنشاء المظاريف.*
- *استخدام Word 2007 في النشر المكتبي لأغراض الفهارس وجداول المحتويات وتقسيم المستندات إلي مقاطع وتجميعها وتجزئتها وإدراج رءوس وتذييل الصفحات وترقيمها.*

تــيســيـــــــر Word 2007

يعتبر كتاب تيسير Word 2007 دليل سهل لتعلـــيم Word 2007 ويغطى الموضوعات الآتية:

- *إنشاء المستند وتعديل محتوياته والتعامل معــه. وإضــافة لمسات جمالية له.*
- *إنشاء الجداول وإجراء تعديلات عليها وتنسيقها.*
- *الدمج البريدي وطباعة الخطابات. والتصحيح التلقائي.*
- *إدراج التاريخ والوقت وإسقاط الأحرف الاستهلالية.*
- *إدراج الصور والرسوم بالمستند.*



المرجع الأساسي لمستخدمي Excel 2007

يشرح هذا الكتاب أحد برامج Office 2007 وهو Excel 2007 ويتناول الكتاب الموضوعات:

- *تصميم وبناء أوراق العمل والتخطيطات البيانيـــة وتنـــسيقها وطباعتها.*
- *استخدام المعادلات والدوال.*
- *التعامل مع الصور والكائنات الرســومية واســتخدام أدوات Excel لرسم الأشكال والكائنات.*
- *تصميم وإنشاء قواعد البيانات وترتيبها وتصفيتها والبحث فيها واستيرادها وتصديرها.*
- *تجميع البيانات وتلخيصها باستخدام الجداول والتخطيطات المحورية.*
- *كيفية تسجيل الماكرو وإعادة تشغيله وتوظيفه لتسهيل أعمالك المتكررة.*
- *نشر البيانات والتخطيطات علي صفحة الويب وإدراج الارتباطات وتحويل البيانـــات إلي صـــفحات ويب تفاعلية.*



تــيســـيـــــــــر Excel 2007

يعتبر كتاب تيسير Excel 2007 دليل سهل لتعليم Excel 2007 لمن لا يجدون الوقت الكافى لقراءة المراجــع المطولـــة ويغطى الموضوعات الآتية:

- *أساسيات برنامج Excel.*
- *كيفية التعامل مع الأوراق وتعديلها وتصحيح الأخطـــاء وتجميع الأعمدة والصفوف.*
- *تنسيق النصوص والبحث والاستبدال وتنسيقات والصيغ واستخدام الدوال.*
- *التخطيطات وقواعد البيانات.*

المرجع الأساسي لمستخدمي Access 2007

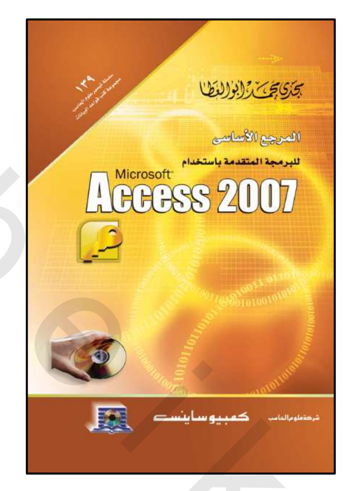
يضع هذا المرجع بين يديك بأسلوب تعليمى منظم أسرار وخبايـا الانطلاق إلى القمة مع Access 2007. ويشمل على:

- *المزايا الجديدة فى Access 2007.*
- *كيفية إنشاء قاعدة بيانات وتعديلها وربطها واستيراد جداولها.*
- *طرق مختلفة للبحث عن البيانات وترتيبها وتصفيتها والاستعلام عنها.*
- *تصميم نماذج وتقارير متقدمة تشتمل علي عناصر تحكم وصور وتبويبات وتستخدم مفاهيم متقدمة في الربط والتضمين.*
- *نشر البيانات والتقـارير علـى صـفحات الويـب. وإدراج الارتباطات التشعبية ومقدمة إلى لغة VBA.*
- *استخدام قاعدة البيانات داخل شبكة اتصالات وكيفية تحويـل تطبيقـات Access إلي تطبيقـات "الخادم/العميل" ومشروعات البيانات (DAP).*

تـيسـيـــر Access 2007

يعتبر كتاب تيسير Access 2007 دليل سهل لتعليم Access 2007 ويغطى الموضوعات الآتية:

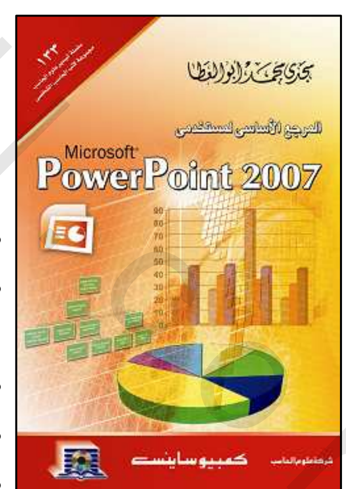
- *مفهوم قواعد البيانات وتنظيم ملفاتها.*
- *المزايا والتحسينات الجديدة فى Access 2007.*
- *إنشاء الجداول وتعديلها. والبحث والاستعلام عن البيانات وإعادة ترتيبها. وتبادل البيانات مع قواعد البيانات والبرامج الأخرى.*
- *إنشاء قواعد البيانات واستعراض محتوياتهـا والـتحكم فى إظهار بياناتها.*
- *تصميم النماذج والتقارير وبطاقات العنونة وربط الجدول.*



البرمجة المتقدمة باستخدام Access 2007

يشرح الكتاب برمجة Access باستخدام Access VBA التي تستخدمها Access 2007 ويشتمل على:

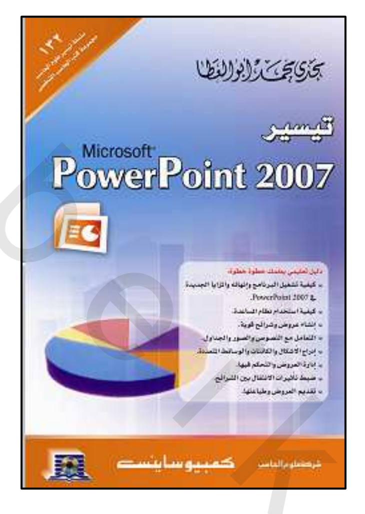
- *مفاهيم البرمجة اللازمة لتصميم وإدارة قواعد البيانات وتشمل أساسيات قواعد البيانات وأنواعها وخطوات تطويرها.*
- *الطرق المختلفة لإنشاء التعبيرات وتعيين قواعد التحقق من الصحة ومعايير الاستعلام.*
- *التعرف على الأحداث والاستجابة لها وفهم كائنات الوصول إلى البيانات.*
- *كيفية تثبيت SQL Server 2005 Express Edition و تحويل تطبيقات Access إلى تطبيقات "الخادم / العميل".*
- *العمل مع مشروعات البيانات (DAP).*



المرجع الأساسى لمستخدمى Power Point 2007

يضع هذا المرجع بين يديك بأسلوب تعليمى منظم أسرار وخبايا الانطلاق إلى القمة مع Power Point 2007. وتساعد هذه الأسرار والنصائح فى تعلم واستخدام Power Point. وتشمل:

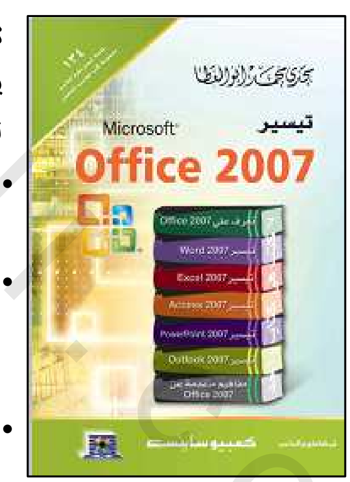
- *إنشاء عروض وشرائح قوية.*
- *إنشاء عروض تشتمل على تقنيات "المالتيمديا" وتشمل الصوت والصورة والحركة.*
- *إضافة النصوص والجداول والرسوم إلي الشرائح .*
- *التحكم في التأثيرات الانتقالية بين الشرائح وتوقيتها.*
- *تسجيل الماكرو وإعادة تشغيله وتوظيفه لتسهيل أداء عروضك.*
- *تطويع Power Point 2007 وتوفيقه ليتناسب استخداماتك الخاصة وكيفية التحكم فى خيارته.*
- *تقديم العروض وتجهيزها لتشغيلها فى مكان آخر أو على جهاز آخر.*



تيسير Power Point 2007

يعتبر كتاب تيسير Power Point 2007 دليل سهل لتعليم Power Point 2007 ويغطى الموضوعات الآتية:

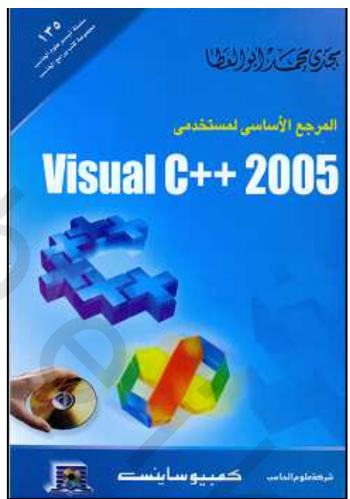
- *كيفية تشغيل البرنامج وإنهائه والمزايا الجديدة فيه.*
- *كيفية استخدام نظام المساعدة وإنشاء عروض وشرائح قوية.*
- *التعامل مع النصوص والصور والجداول.*
- *إدراج الأشكال والكائنات والوسائط المتعددة.*
- *ضبط تأثيرات الانتقال بين الشرائح وتقديم العروض وطباعتها.*



تيسير Office 2007

يعتبر كتاب Office 2007 دليل سهل لمن لا يجدون الوقت الكافى لقراءة المراجع المطولة ويغطى الموضوعات الآتية:

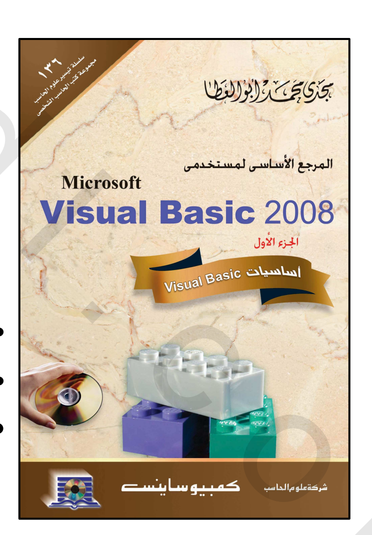
- *المفاهيم العامة والأساسية لبرامج **Office 2007** والتغيير الذي طرأ علي الواجهات*
- *إنشاء مستندات باستخدام **Word** وتنسيقها وإضافة لمسات جمالية تشمل الخطوط والظلال والحدود والأعمدة والجداول والصور.*
- *إنشاء أوراق عمل باستخدام **Excel** وتجميلها وتنسيق محتوياتها،*
- *إنشاء واستخدام قواعد البيانات باستخدام **Access**.*
- *تصميم شرائح العرض وتنسيقها وعرضها باستخدام **Power Point** .*
- *تنظيم مواعيدك وإرسال واستقبال البريد الإلكتروني والتخطيط للاجتماعات باستخدام **Outlook** .*



المرجع الأساسي لمستخدمي Visual C++ 2005

يضع هذا المرجع بين يديك بأسلوب تعليمي منظم أسـرار وخبايا الانطلاق إلى القمة مع Visual C++ 2005 ويشمل على:

- *فتح بيئة تطوير Visual Studio 2005 والتعرف على مكوناتها واستخدمتها لإنشاء التطبيقات الجديدة.*
- *إنشاء المربعات الحوارية بنوعيها واستخدام أدوات التحكم المختلفة لتبادل البيانات بين المستخدمين والتطبيق إلي جانب التحقق من صحة البيانات.*
- *إنشاء الصور والرموز ورسم الخطوط والأشكال المركبة عن طريق أقلام الرسم وفرش الألوان واستخدامها داخل المربعات الحوارية.*

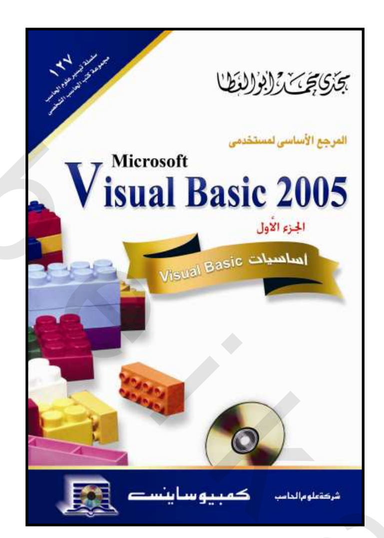


المرجع الاساسي لمستخدمي Visual Basic 2008

يتناول هذا المرجع بالتفصيل كل ما يخص Visual Basic 2008 ويبين كيفية استخدام الإمكانات التي توفرها Visual Basic لتصبح في النهاية مبرمجا جيداً يقع هذا المرجع في ثلاثة أجزاء على النحو التالي:

- *الجزء الأول : أساسيات Visual Basic 2008*
- *الجزء الثاني : برمجة Visual Basic 2008*
- *الجزء الثالث : البرمجة المتقدمة وقواعد البيانات*

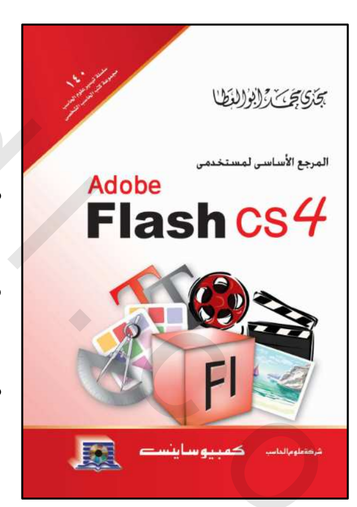
المرجع الأساسي لمستخدمي Visual Basic 2005



يتناول هذا المرجع بالتفصيل كل ما يخـــص Visual Basic 2005 ويبين كيفية استخدام الإمكانات التى توفرها Visual Basic لتصبح فى النهاية مبرمجا جيداً يقع هذا المرجـــع فى ثلاثة أجزاء على النحو التالى:

- *الجزء الأول : أساسيات Visual Basic 2005*
- *الجزء الثانى : برمجة Visual Basic 2005*
- *الجزء الثالث : البرمجة المتقدمة وقواعد البيانات*

المرجع الأساسي لمستخدمي Flash CS4



يشرح هذا الكتاب واحداً من أهم بـــرامج الرســـوم وتـــصميم صفحات ومواقع الويب وهو برنامج Flash ويشرح ما يلى:

- أهمية استخدام Flash فى إنشاء تطبيقات الرسوم وتـــصميم مواقع الويب. والسمات الجديدة فى *Flash CS4*
- كيفيـــة اســـتخدام الرمـــوز Symbols والحـــالات Instances.والتحكم فى سماتها المختلفة.
- استخدام الطبقات فى تنظيم عناصر التطبيق وإنشاء أكثر من حدث فى نفس الوقت. إنشاء الرسوم المتحركة لإضفاء المزيد من المتعة على تطبيقاتك.
- استخدام المشاهد Scenes لتقسيم تطبيقك إلى صفحات مستقلة.
- نشر أفلامك وتوزيعا بالتنسيقات المختلفة.

المرجع الأساسي لمستخدمي Photoshop CS4

يشرح هذا البرنامج واحدًا من أهم وأشهر برامج معالجة الرسوم والصور وفى هذا الكتاب ستجد معلومات وافية عن:

- مفاهيم التحكم فى الصور وأنواعها وطباعتها وإدارة ملفاتها. وأيضا العمل مع أجزاء مختارة من الصور.
- استعادة الصور القديمة وإصلاحها وضبطها.
- استخدام الفلاتر والمؤثرات الخاصة.
- تعديل وتحسين الصور وإضافة مؤثرات عليها.
- إنشاء صفحة الويب من البداية. وإضافة تأثيرات مختلفة وتأثيرات حركية لها.
- كيفية استخدام الإجراءات وإنشاء صور تفاعلية.



المرجع الأساسي لمستخدمي Word 2003

يشرح هذا الكتاب واحد من أهم برامج مجموعة Office 2003 وهو Word 2003، ويتناول الكتاب الموضوعات التالية:

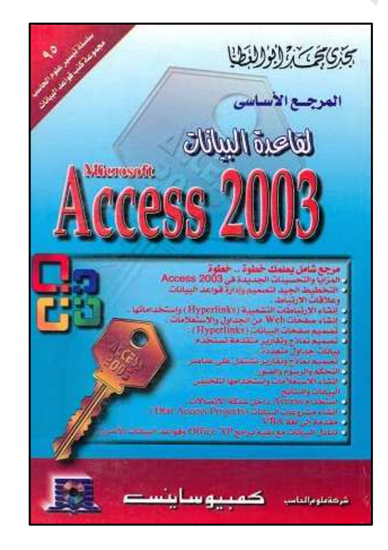
- *المزايا الجديدة فى Word 2003.*
- *مفاهيم تحرير المستندات وتنسيقها وتعديلها وتصحيحها وطباعتها.*
- *تصميم مستندات تشتمل على الصور والرسوم ومربعات النص. وكيفية إنشاء المظاريف.*
- *التعامل مع المستندات الكبيرة وتقسيم المستند إلى مقاطع وإدراج التعليقات التوضيحية والإشارات المرجعية.*



المرجع الأساسى لمستخدمي Excel 2003.

يشرح هذا الكتاب أحد برامج Office 2003 وهو Excel 2003 ويتناول الكتاب الموضوعات التالية:

- *تصميم وإنشاء قواعد البيانات وترتيبها وتصفيتها والبحث فيها.*
- *استخدام المعادلات والدوال.*
- *تصميم وبناء أوراق العمل والتخطيطات البيانية وتنسيقها وطباعتها.*
- *تجميع البيانات وتلخيصها باستخدام الجداول والتخطيطات المحورية.*
- *التعامل مع الصور والكائنات الرسومية واستخدام أدوات Excel لرسم الأشكال والكائنات.*



المرجع الأساسي لمستخدمي Access 2003

يضع هذا المرجع بين يديك بأسلوب تعليمي منظم أسرار وخبايا الانطلاق إلى القمة مع Access 2003. ويشمل على:

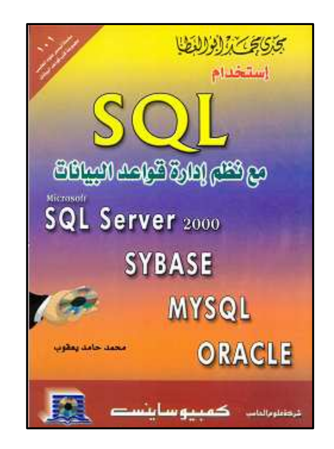
- *المزايا الجديدة فى Access 2003.*
- *طرق مختلفة للبحث والاستعلام وتعريف الاستعلام الإجرائي*
- *نشر البيانات والتقارير على صفحات الويب. وإدراج الارتباطات التشعبية ومقدمة إلى لغة VBA.*
- *تعريف المبادئ الأساسية لتأمين قواعد البيانات. وخصائص مشروعات البيانات والسمات الجديدة فى كل من MSDE و SQL Server.*



تيسير Office 2003

يعتبر كتاب Office 2003 دليل سهل لمن لا يجدون الوقت الكافى لقراءة المراجع المطولة ويغطى الموضوعات الآتية:

- *المفاهيم العامة والأساسية لبرامج* **Office 2003** .
- *إنشاء مستندات باستخدام* **Word** *وتنسيقها وإضافة لمسات جمالية تشمل الخطوط والظلال والحدود والأعمدة والجداول والصور.*
- *إنشاء أوراق عمل باستخدام* **Excel** *وتجميلها وتنسيق محتوياتها،*
- *إنشاء واستخدام قواعد البيانات باستخدام* **Access**.
- *تصميم شرائح العرض وتنسيقها وعرضها باستخدام* **Power Point**.
- *تنظيم مواعيدك وإرسال واستقبال البريد الإلكتروني والتخطيط للاجتماعات باستخدام* **Outlook** .



استخدام نظم إدارة قواعد البيانات SQL

يضع هذا الكتاب بين يديك كل ما تحتاج إليه لكى تستخدم بكفاءة لغة SQL من أربعة نظم إدارة قواعد البيانات الشهيرة وهى Oracle–My SQL و SQL Server 2000 وSybase،سوف تجد فى هذا الكتاب معلومات وافية تشمل:

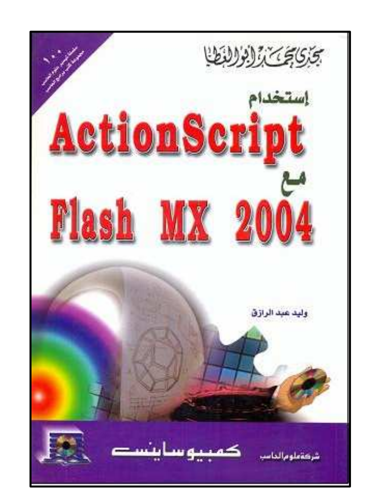
- *مقدمة عن نظم إدارة قواعد البيانات* **RDBMS** *وكيفية تثبيتها والتعامل معها.*
- *معالجة الجداول وقواعد البيانات ويشمل ربط الجداول وإنشائها والضوابط التى تضمن سلامة البيانات.*
- *مفاهيم متقدمة تشمل استخدام استعلام آخر والتحكم فى وحدة العمل واستخدام الجداول التخيلية وفهرسة البيانات.،*
- *مشروعات تطبيقية عن استخدام* **SQL** *مع كل من* **JAVA** *و* **C#NET**.



تصميم صفحات الإنترنت

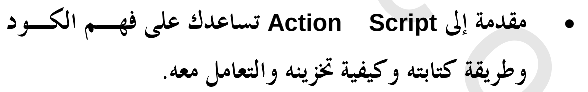
يعتمد هذا الكتاب على مبدأ التدرج فى التعليم من الأسهل إلى الأصعب حيث يبدأ بشرح برنامج FrontPage لإعداد صفحة ويب ثم شرحنا لغة البرمجة الحديثة HTML، فى هذا الكتاب ستجد معلومات وافية عن:

- تطوير صفحات ويب جذابة تشتمل على النصوص والصور والارتباطات التشعبية والرسوم والقوائم باستخدام برنامج FrontPage.
- التعرف على لغة HTML وضرورتها وكيفية استخدامها والأدوات التى تلزمك للتعامل معه.
- تطوير صفحات باستخدام HYML بشكل جذاب تشمل كل ما تستخدمه فى مواقع الويب مثل النصوص والصور والرسوم والقوائم والارتباطات التشعبية.
- تطوير صفحات الإنترنت باستخدام HTML تحتوى على النماذج والجداول.



استخدام Action Script مع Flash MX 2004

يخاطب هذا الكتاب من لهم خبرة باستخدام Flash MX 2004 ويريدون الحصول على مزايا تجعل الأفلام التى يحصلون عليها والمواقع التى يقومون بتصميمها أسهل فى التصميم وأكثر جاذبية فى الأداء.يتناول الكتاب المفاهيم التى تسهل لك كتابة واستخدام كود Action Script وتشمل :



- مقدمة إلى Action Script تساعدك على فهم الكود وطريقة كتابته وكيفية تخزينه والتعامل معه.
- استخدام المتغيرات Variables والأنواع المختلفة للبيانات وكيفية التحويل بينها.
- استخدام الدوال Functions والأحداث Events لتنفيذ مهام معينة أو سبق تحديدها.